Handbuch zur Serverkonfiguration für ESX Server 3

ESX Server 3.5 und VirtualCenter 2.5

vmware®

Handbuch zur Serverkonfiguration für ESX Server 3
Überarbeitung: 20080410
Artikelnummer: VI-DEU-Q208-479

Die neueste technische Dokumentation finden Sie auf unserer Webseite unter:

http://www.vmware.com/support/

Auf der VMware-Webseite finden Sie auch die neuesten Produktaktualisierungen.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie diese bitte an:

docfeedback@vmware.com

© 2006-2008 VMware, Inc. Alle Rechte vorbehalten. Geschützt durch mindestens eines der US-Patente Nr. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156, 6,795,966, 6,880,022, 6,944,699, 6,961,806, 6,961,941, 7,069,413, 7,082,598, 7,089,377, 7,111,086, 7,111,145, 7,117,481, 7,149,843, 7,155,558, 7,222,221, 7,260,815, 7,260,820, 7,269,683, 7,275,136, 7,277,998, 7,277,999, 7,278,030, 7,281,102 und 7,290,253. weitere Patente sind angemeldet.

VMware, das VMware-Logo und -Design, Virtual SMP und VMotion sind eingetragene Marken oder Marken der VMware, Inc. in den USA und/oder anderen Ländern. Alle anderen in diesem Dokument erwähnten Bezeichnungen und Namen sind unter Umständen markenrechtlich geschützt.

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Inhalt

Über dieses Handbuch 9

1 Einführung 13
Netzwerk 14
Speicher 14
Sicherheit 15
Anhänge 16

Netzwerk

2 Netzwerke 19
Übersicht über Netzwerkkonzepte 20
Virtuelle Switches 22
Portgruppen 24
Aktivieren von Netzwerkdiensten 24
Anzeigen der Netzwerkinformationen im VI-Client 25
Konfiguration virtueller Netzwerke für virtuelle Maschinen 27
Netzwerkkonfiguration des VMkernels 30
TCP/IP-Stapel auf VMkernel-Ebene 30
Aspekte und Richtlinien für die Konfiguration 31
Konfiguration der Servicekonsole 34
Grundlegende Konfigurationsaufgaben für die Servicekonsole 34
Verwenden von DHCP für die Servicekonsole 39

3 Erweiterte Netzwerkthemen 41
Eigenschaften und Richtlinien für virtuelle Switches 42
Eigenschaften virtueller Switches 42
Richtlinien für virtuelle Switches 51
Konfigurieren der Portgruppe 60
DNS und Routing 64
TCP-Segmentierungs-Offload und Jumbo-Frames 65

Aktivieren von TSO 65
Aktivieren von Jumbo-Frames 67
NetQueue und Netzwerkleistung 68
Einrichten von MAC-Adressen 69
Generierung von MAC-Adressen 69
Festlegen von MAC-Adressen 70
Verwenden von MAC-Adressen 71
Optimale Vorgehensweisen und Tipps für Netzwerke 71
Optimale Vorgehensweisen für Netzwerke 72
Netzwerktipps 73

4 Netzwerkszenarien und Problemlösung 75
Netzwerkkonfiguration für Software-iSCSI-Speicher 76
Konfigurieren des Netzwerks auf Blade-Servern 81
Fehlerbehebung 85
Fehlerbehebung bei der Vernetzung der Servicekonsole 85
Fehlerbehebung bei der Netzwerkadapterkonfiguration 86
Fehlerbehebung bei der Konfiguration physischer Switches 86
Fehlerbehebung bei der Portgruppenkonfiguration 87

Speicher

5 Einführung in die Speicherung 91
Speicher – Übersicht 92
Physische Speichertypen 93
Lokaler Speicher 93
Netzwerkspeicher 94
Unterstützte Speicheradapter 95
Datenspeicher 95
VMFS-Datenspeicher 96
NFS-Datenspeicher 100
Speicherzugriff durch virtuelle Maschinen 100
Vergleich der Speichertypen 102
Anzeigen der Speicherinformationen im VMware Infrastructure-Client 102
Anzeigen von Datenspeichern 103
Anzeigen von Speicheradaptern 104
Grundlegendes zur Benennung von Speichergeräten in der Anzeige 105
Konfigurieren und Verwalten von Speichern 106

6 Speicherkonfiguration 109
Lokaler Speicher 110
Hinzufügen von lokalem Speicher 110
Fibre-Channel-Speicher 113
Hinzufügen von Fibre-Channel-Speicher 114
iSCSI-Speicher 116
iSCSI-Initiatoren 116
Benennungskonventionen 117
Erkennungsmethoden 118
iSCSI-Sicherheit 118
Konfigurieren von Hardware-iSCSI-Initiatoren und -Speicher 119
Konfigurieren von Software-iSCSI-Initiatoren und Speicher 127
Starten einer erneuten Prüfung 134
Network Attached Storage (NAS) 135
Verwendung von NFS durch virtuelle Maschinen 135
NFS-Volumes und delegierte Benutzer für virtuelle Maschine 136
Konfigurieren von ESX Server 3 für den Zugriff auf NFS-Volumes 137
Erstellen eines NFS-basierten Datenspeichers 137
Erstellen einer Diagnosepartition 138

7 Speicherverwaltung 141
Verwalten von Datenspeichern 142
Bearbeiten von VMFS-Datenspeichern 143
Aktualisieren von Datenspeichern 143
Ändern des Namens von Datenspeichern 144
Hinzufügen von Erweiterungen zu Datenspeichern 145
Verwalten mehrerer Pfade 146
Multipathing mit lokalem Speicher und Fibre-Channel-SANs 147
Multipathing mit iSCSI-SAN 148
Anzeigen des aktiven Multipathing-Status 149
Einrichten von Multipathing-Richtlinien für LUNs 151
Deaktivieren von Pfaden 153
Die vmkfstools-Befehle 154

8 Raw-Gerätezuordnung 155
Wissenswertes zur Raw-Gerätezuordnung 156
Vorteile von Raw-Gerätezuordnungen 157
Einschränkungen der Raw-Gerätezuordnung 160
Raw-Gerätezuordnungseigenschaften 161
Vergleich des virtuellen und mit dem physischen Kompatibilitätsmodus 161

Dynamische Namensauflösung 163
Raw-Gerätezuordnung für Cluster aus virtuellen Maschinen 164
Vergleich der Raw-Gerätezuordnung mit anderen Möglichkeiten des SCSI-Gerätezugriffs 165
Verwalten zugeordneter LUNs 165
VMware Infrastructure-Client 165
Das Dienstprogramm vmkfstools 169
Dateisystemfunktionen 169

Sicherheit

9 Sicherheit für ESX Server 3-Systeme 173
Architektur und Sicherheitsfunktionen von ESX Server 3 173
Sicherheit und die Virtualisierungsebene 174
Sicherheit und virtuelle Maschinen 174
Sicherheit und die Servicekonsole 177
Sicherheit und die virtuelle Netzwerkebene 179
Sonstige Quellen und Informationen zur Sicherheit 186

10 Absichern einer ESX Server 3-Konfiguration 187
Absichern des Netzwerks mit Firewalls 187
Firewalls in Konfigurationen mit einem VirtualCenter Server 189
Firewalls für Konfigurationen ohne VirtualCenter Server 191
TCP- und UDP-Ports für den Verwaltungszugriff 193
Herstellen einer Verbindung mit einem VirtualCenter Server über eine Firewall 195
Herstellen einer Verbindung mit der VM-Konsole über eine Firewall 196
Verbinden von ESX Server 3-Hosts über Firewalls 198
Öffnen von Firewallports für unterstützte Dienste und Verwaltungs-Agenten 198
Absichern virtueller Maschinen durch VLANs 203
Sicherheitsempfehlungen für vSwitches und VLANs 207
Schutz durch virtuelle Switches in VLANs 209
Absichern der Ports virtueller Switches 211
Absichern von iSCSI-Speicher 214
Absichern von iSCSI-Geräten über Authentifizierung 214
Schützen eines iSCSI-SAN 218

11 Authentifizierung und Benutzerverwaltung 221
Absichern von ESX Server 3 über Authentifizierung und Berechtigungen 221
Informationen zu Benutzern, Gruppen, Berechtigungen und Rollen 223
Verwalten von Benutzern und Gruppen auf ESX Server 3-Hosts 230
Verschlüsselungs- und Sicherheitszertifikate für ESX Server 3 236
Hinzufügen von Zertifikaten und Ändern der Web-Proxyeinstellungen von ESX Server 3 238
Erneutes Erzeugen von Zertifikaten 242
Delegierte VM-Benutzer für NFS-Speicher 242

12 Sicherheit der Servicekonsole 247
Allgemeine Sicherheitsempfehlungen 248
Anmelden an der Servicekonsole 249
Konfiguration der Servicekonsolen-Firewall 249
Ändern der Sicherheitsstufe der Servicekonsole 250
Freigeben und Blockieren von Ports in der Servicekonsolen-Firewall 252
Kennwortbeschränkungen 254
Kennwortverwendungsdauer 255
Kennwortkomplexität 256
Ändern des Kennwort-Plug-Ins 260
Schlüsselqualität 262
setuid- und setgid-Anwendungen 263
setuid-Standardanwendungen 263
setgid-Standardanwendungen 265
SSH-Sicherheit 265
Sicherheitspatches und Software zum Suchen nach Sicherheitslücken 267

13 Empfehlungen für den Schutz von Implementierungen 269
Sicherheitsmaßnahmen für gängige ESX Server 3-Implementierungen 269
Implementierung „für einen Kunden“ 270
Eingeschränkte Implementierung für mehrere Kunden 272
Beschränkte Implementierung für mehrere Kunden 274
Empfehlungen für virtuelle Maschinen 276
Installieren von Antivirensoftware 276
Deaktivieren von Kopier- und Einfügevorgängen zwischen Gastbetriebssystem und Remotekonsole 277
Entfernung überflüssiger Hardwaregeräte 278
Beschränken von Schreibvorgängen des Gastbetriebssystems in den Hostspeicher 280
Konfigurieren der Protokollierungsebenen für das Gastbetriebssystem 283

Anhänge

A Befehle für den technischen Support von ESX Server 3 291
Andere Befehle 298

B Verwenden von „vmkfstools“ 299
vmkfstools-Befehlssyntax 300
vmkfstools-Optionen 301
Unteroption -v 301
Dateisystemoptionen 301
Optionen für virtuelle Festplatten 305
Verwalten der SCSI-Reservierungen von LUNs 312

Index 313

Über dieses Handbuch

In diesem *Handbuch zur Serverkonfiguration für ESX Server 3* finden Sie Informationen zur Konfiguration von ESX Server 3 (z. B. zur Erstellung virtueller Switches und Ports sowie zur Einrichtung des Netzwerks für virtuelle Maschinen, VMotion, IP-Speicher und die Servicekonsole. Es enthält ebenfalls Informationen zum Konfigurieren des Dateisystems und verschiedener Speichertypen, wie zum Beispiel iSCSI, Fibre-Channel usw. Zum Schutz Ihrer ESX Server 3-Installation enthält das Handbuch umfassende Informationen zu den in ESX Server 3 enthaltenen Sicherheitsfunktionen und Maßnahmen, die zum Schutz vor Angriffen ergriffen werden können. Ferner enthalten ist eine Liste mit technischen Unterstützungsbefehlen für ESX Server 3 und deren Entsprechung im VI-Client sowie eine Beschreibung des Dienstprogramms `vmkfstools`.

Das *Handbuch zur Serverkonfiguration für ESX Server 3* gilt für ESX Server 3.5. Informationen zu ESX Server 3i, Version 3.5, finden Sie unter http://www.vmware.com/support/pubs/vi_pubs.html.

Zur Vereinfachung der Erläuterung werden in diesem Buch die folgenden Produktbenennungskonventionen befolgt:

- Für Themen, die für ESX Server 3.5 spezifisch sind, wird in diesem Buch der Begriff „ESX Server 3“ verwendet.
- Für Themen, die für ESX Server 3i, Version 3.5, spezifisch sind, wird in diesem Buch der Begriff „ESX Server 3i“ verwendet.
- Für Themen, die für beide Produkte gelten, wird in diesem Buch der Begriff „ESX Server“ verwendet.

- Wenn die Bestimmung einer bestimmten Version für die Erläuterung wichtig ist, wird in diesem Buch für das jeweilige Produkt der folgende Name samt Version angegeben.
- Wenn sich die Erläuterung auf alle Versionen von ESX Server for VMware® Infrastructure 3 bezieht, wird in diesem Buch der Begriff „ESX Server 3.x“ verwendet.

Zielgruppe

Dieses Handbuch richtet sich an alle Benutzer, die ESX Server 3 installieren, verwenden oder aktualisieren möchten. Die Informationen in diesem Handbuch wurden für erfahrene Administratoren von Windows- oder Linux-Systemen geschrieben, die mit der Technologie virtueller Maschinen und Datencenter-Vorgängen vertraut sind.

Feedback zu diesem Dokument

VMware freut sich über Ihre Vorschläge zum Verbessern der Dokumentation. Bitte senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

Dokumentation zu VMware Infrastructure

Die Dokumentation zu VMware Infrastructure umfasst die kombinierte Dokumentation zu VMware VirtualCenter und ESX Server.

In Abbildungen verwendete Abkürzungen

In den Grafiken in diesem Handbuch werden die in Tabelle 1 aufgeführten Abkürzungen verwendet.

Tabelle 1. Abkürzungen

Abkürzung	Beschreibung
VC	VirtualCenter
VM	Virtuelle Maschine
VI Client	VMware Infrastructure-Client
server	VirtualCenter Server
database	VirtualCenter-Datenbank
host*n*	Verwaltete VirtualCenter-Hosts
VM#	Virtuelle Maschinen auf einem verwalteten Host

Tabelle 1. Abkürzungen (Fortsetzung)

Abkürzung	Beschreibung
user#	Benutzer mit Zugriffsberechtigungen
dsk#	Speicherfestplatte für den verwalteten Host
datastore	Speicher für den verwalteten Host
SAN	Datenspeicher vom Typ Storage Area Network, der von verwalteten Hosts gemeinsam genutzt wird
tmplt	Vorlage

Technischer Support und Schulungsressourcen

In den folgenden Abschnitten werden die verfügbaren technischen Supportressourcen beschrieben. Unter der folgenden Adresse haben Sie Zugang zu den neuesten Versionen dieses Handbuchs und anderen Büchern:

http://www.vmware.com/support/pubs

Online- und Telefon support

Im Online-Support können Sie technische Unterstützung anfordern, Ihre Produkt- und Vertragsdaten abrufen und Produkte registrieren. Weitere Informationen finden Sie unter http://www.vmware.com/support.

Kunden mit entsprechenden Support-Verträgen erhalten über den telefonischen Support die schnellste Hilfe bei Problemen der Prioritätsstufe 1. Weitere Informationen finden Sie unter http://www.vmware.com/support/phone_support.html.

Support-Angebote

VMware stellt ein umfangreiches Support-Angebot bereit, um Ihre geschäftlichen Anforderungen zu erfüllen. Weitere Informationen finden Sie unter http://www.vmware.com/support/services.

VMware Education Services

Die VMware-Kurse umfassen umfangreiche praktische Übungen, Fallbeispiele und Kursmaterialien, die zur Verwendung als Referenztools bei der praktischen Arbeit vorgesehen sind. Weitere Informationen zu den VMware Education Services finden Sie unter http://mylearn1.vmware.com/mgrreg/index.cfm.

Einführung 1

Im *Handbuch zur Serverkonfiguration für ESX Server 3* werden die Aufgaben beschrieben, die Sie zur Konfiguration des ESX Server 3-Hostnetzwerks, des Speichers und der Sicherheitsfunktionen durchführen müssen. Außerdem enthält es Übersichten, Empfehlungen und Grundlagenerläuterungen, die Ihnen beim Verständnis dieser Aufgaben und bei der Implementierung eines ESX Server 3-Hosts helfen, der Ihren Anforderungen entspricht. Bevor Sie das *Handbuch zur Serverkonfiguration für ESX Server 3* durchlesen, machen Sie sich mit der *Einführung in die virtuelle Infrastruktur* vertraut, in der Sie eine Übersicht über die Systemarchitektur sowie die physischen und virtuellen Geräte erhalten, aus denen sich ein VMware Infrastructure-System zusammensetzt.

Diese Einführung bietet eine Übersicht über den Inhalt des vorliegenden Handbuchs, sodass Sie die benötigten Informationen schneller auffinden können. In diesem Handbuch werden die folgenden Themen behandelt:

- Netzwerkkonfigurationen für ESX Server 3
- Speicherkonfigurationen für ESX Server 3
- Sicherheitsfunktionen von ESX Server 3
- ESX Server 3-Befehlsreferenz
- Der Befehl `vmkfstools`

Netzwerk

Die Kapitel zu ESX Server 3-Netzwerken bieten Ihnen eine grundlegende Vermittlung der Konzepte physischer und virtueller Netzwerke, eine Beschreibung der Basisaufgaben, die Sie erfüllen müssen, um die Netzwerkverbindungen Ihres ESX Server-Hosts herzustellen, sowie eine Erläuterung erweiterter Netzwerkthemen und -aufgaben. Der Abschnitt zu Netzwerken enthält die folgenden Kapitel:

- Netzwerke – Stellt Netzwerkkonzepte vor und führt durch Routineaufgaben, die zur Konfiguration eines Netzwerks auf dem ESX Server 3-Host notwendig sind.
- Erweiterte Netzwerkthemen – Behandelt erweiterte Netzwerkaufgaben, wie zum Beispiel die Einrichtung von MAC-Adressen, die Bearbeitung virtueller Switches und Ports und das DNS-Routing. Darüber hinaus erhalten Sie Tipps, wie Sie die Effizienz der Netzwerkkonfiguration steigern können.
- Netzwerkszenarien und Problemlösung – Beschreibt allgemeine Netzwerkkonfigurations- und Problemlösungsszenarien.

Speicher

In den Kapiteln zu den Speichereinstellungen für ESX Server 3 werden Speichervorgänge grundlegend vermittelt. Außerdem werden die grundlegenden erforderlichen Aufgaben zum Konfigurieren und Verwalten des Speichers für ESX Server 3 beschrieben und das Einrichten von Raw-Gerätezuordnungen erläutert. Der Abschnitt zu Speichereinstellungen enthält die folgenden Kapitel:

- Einführung in die Speicherung – Stellt die Speichertypen vor, die für den ESX Server 3-Host konfiguriert werden können.
- Speicherkonfiguration – Erläutert die Konfiguration von lokalem SCSI-Speicher, Fibre-Channel-Speicher und iSCSI-Speicher. Darüber hinaus werden der VMFS-Speicher (Virtual Machine File System) und NAS-Speicher (Network-Attached Storage, über das Netzwerk angebundener Speicher) behandelt.
- Speicherverwaltung – Erläutert die Verwaltung bestehender Datenspeicher und der Dateisysteme, aus denen die Datenspeicher bestehen.
- Raw-Gerätezuordnung – Behandelt die Raw-Gerätezuordnung, die Konfiguration dieses Speichertyps und die Verwaltung von Raw-Gerätezuordnungen durch Einrichtung von Multipathing, Failover usw.

Sicherheit

In den Kapiteln zur ESX Server 3-Sicherheit werden Sicherheitsmaßnahmen erläutert, die von VMware in ESX Server 3 integriert wurden. Außerdem werden Maßnahmen beschrieben, mit denen Sie den ESX Server 3-Host vor Sicherheitsrisiken schützen können. Zu diesen Maßnahmen zählen das Einrichten von Firewalls, die Ausnutzung der Sicherheitsfunktionen virtueller Switches sowie das Konfigurieren von Benutzerauthentifizierungen und -berechtigungen. Der Abschnitt zur Sicherheit enthält die folgenden Kapitel:

- Sicherheit für ESX Server 3-Systeme – Stellt die ESX Server 3-Funktionen, mit denen Sie die Umgebung für Ihre Daten sichern können, und eine sicherheitsbezogene Übersicht über den Systemaufbau vor.
- Absichern einer ESX Server 3-Konfiguration – Erläutert die Konfiguration von Firewallports für ESX Server 3-Hosts und VMware VirtualCenter, die Verwendung von virtuellen Switches und VLANs zur Sicherstellung der Netzwerkisolierung für virtuelle Maschinen und die Absicherung von iSCSI-Speicher.
- Authentifizierung und Benutzerverwaltung – Erläutert die Einrichtung von Benutzern, Gruppen, Zugriffsrechten und Rollen zur Steuerung des Zugriffs auf ESX Server 3-Hosts und VirtualCenter. Außerdem werden die Verschlüsselung und das Delegieren von Benutzern beschrieben.
- Sicherheit der Servicekonsole – Behandelt die Sicherheitsfunktionen der Servicekonsole und die Konfiguration dieser Funktionen.
- Empfehlungen für den Schutz von Implementierungen – Führt einige Beispielimplementierungen auf, um zu verdeutlichen, welche Probleme bei der Implementierung von ESX Server 3 beachtet werden müssen. Darüber hinaus werden Maßnahmen beschrieben, mit denen Sie virtuelle Maschinen noch weiter absichern können.

Anhänge

Das *Handbuch zur Serverkonfiguration für ESX Server 3* enthält Anhänge, in denen Sie spezielle Informationen finden, die beim Konfigurieren eines ESX Server 3-Hosts hilfreich sein können.

- Befehle für den technischen Support von ESX Server 3 – Behandelt die Konfigurationsbefehle für ESX Server 3, die über eine Befehlszeilenshell wie SSH eingegeben werden können. Zwar stehen Ihnen diese Befehle zur Verfügung, es handelt sich jedoch dabei nicht um eine API, über die Skripts erstellt werden können. Diese Befehle können geändert werden, und VMware unterstützt keine Anwendungen und Skripts, die sich auf Befehle für die ESX Server 3-Konfiguration stützen. In diesem Anhang finden Sie die Entsprechungen dieser Befehle für den VMware Infrastructure-Client.
- Verwenden von „vmkfstools“ – Behandelt das Dienstprogramm `vmkfstools`, mit dem Sie Verwaltungs- und Migrationsaufgaben für iSCSI-Festplatten durchführen können.

Netzwerk

Netzwerke 2

In diesem Kapitel werden die Netzwerkgrundlagen für ESX Server 3-Umgebungen sowie die Einrichtung und Konfiguration von Netzwerken in virtuellen Infrastrukturen erläutert.

Mit dem VMware Infrastructure (VI)-Client können Sie eine Netzwerkanbindung herstellen. Dabei gibt es drei Kategorien, die die drei Typen von Netzwerkdiensten widerspiegeln:

- Virtuelle Maschinen
- VMkernel
- Servicekonsole

In diesem Kapitel werden folgende Themen behandelt:

- „Übersicht über Netzwerkkonzepte“ auf Seite 20
- „Aktivieren von Netzwerkdiensten“ auf Seite 24
- „Anzeigen der Netzwerkinformationen im VI-Client“ auf Seite 25
- „Konfiguration virtueller Netzwerke für virtuelle Maschinen“ auf Seite 27
- „Netzwerkkonfiguration des VMkernels“ auf Seite 30
- „Konfiguration der Servicekonsole“ auf Seite 34

Übersicht über Netzwerkkonzepte

Es sind bestimmte Grundlagen notwendig, um virtuelle Netzwerke vollständig zu verstehen. Wenn Sie bisher noch nicht mit ESX Server 3 gearbeitet haben, empfiehlt VMware Ihnen dringend die Lektüre dieses Abschnittes.

Ein *physisches Netzwerk* ist ein Netzwerk aus physischen Computern, die so miteinander verbunden sind, dass sie untereinander Daten empfangen und versenden können. VMware ESX Server 3 wird auf einem physischen Computer ausgeführt.

Ein *virtuelles Netzwerk* ist ein Netzwerk aus virtuellen Computern (virtuellen Maschinen), die auf einem einzelnen physischen Computer ausgeführt werden. Diese sind logisch miteinander verbunden, sodass sie untereinander Daten empfangen und versenden können. Virtuelle Maschinen können an die virtuellen Netzwerke angeschlossen werden, die Sie beim Hinzufügen eines Netzwerks erstellen. Jedes einzelne virtuelle Netzwerk verfügt über einen virtuellen Switch. Ein virtuelles Netzwerk kann an ein physisches Netzwerk angeschlossen werden, indem mindestens ein physischer Ethernet-Adapter (auch Uplink-Adapter genannt) dem virtuellen Switch des virtuellen Netzwerks zugewiesen wird. Wenn dem virtuellen Switch kein Uplink-Adapter zugewiesen wurde, ist der Datenverkehr im virtuellen Netzwerk auf den physischen Hostcomputer beschränkt. Wenn dem virtuellen Switch mindestens ein Uplink-Adapter zugewiesen wurde, können die virtuellen Maschinen, die an dieses virtuelle Netzwerk angeschlossen sind, auch auf die physischen Netzwerke zugreifen, die an den oder die Uplink-Adapter angeschlossen sind.

Ein *physischer Ethernet-Switch* verwaltet den Netzwerkdatenverkehr zwischen den Computern im physischen Netzwerk. Ein Switch verfügt über mehrere Ports. Jeder dieser Ports kann an einen anderen Computer oder Switch im Netzwerk angeschlossen sein. Jeder Port kann je nach Bedarf des angeschlossenen Computers so konfiguriert werden, dass er sich auf eine bestimmte Art verhält. Der Switch stellt fest, welche Hosts an welche seiner Ports angeschlossen sind, und verwendet diese Informationen, um Daten an den entsprechenden richtigen physischen Computer weiterzuleiten. Switches bilden den Kern eines physischen Netzwerks. Es können mehrere Switches zusammengeschlossen werden, um größere Netzwerke zu bilden.

Ein virtueller Switch, ein sog. *vSwitch*, funktioniert ähnlich wie ein physischer Ethernet-Switch. Er weiß, welche virtuellen Maschinen logisch an welche virtuellen Ports angeschlossen sind, und verwendet diese Informationen, um Daten an die entsprechende richtige virtuellen Maschine weiterzuleiten. Ein vSwitch kann über physische Ethernet-Adapter (auch Uplink-Adapter) an physische Switches angeschlossen werden, um virtuelle und physische Netzwerke zu verbinden. Diese Verbindung ähnelt der Vernetzung physischer Switches zur Bildung größerer Netzwerke. Obwohl ein vSwitch ähnlich wie ein physischer Switch funktioniert,

verfügt er nicht über alle erweiterten Funktionsmerkmale eines physischen Switches. Siehe „Virtuelle Switches“ auf Seite 22.

Eine *Portgruppe* legt Port-Konfigurationsoptionen, z. B. Bandbreitenbeschränkungen oder VLAN-Tagging-Richtlinien, für jeden Port in der Portgruppe fest. Netzwerkdienste werden über Portgruppen an vSwitches angeschlossen. Portgruppen definieren, wie eine Verbindung über den vSwitch an das physische Netzwerk erfolgt. Normalerweise wird einem vSwitch mindestens eine Portgruppe zugewiesen. Siehe „Portgruppen“ auf Seite 24.

NIC-Gruppierung tritt auf, wenn einem vSwitch mehrere Uplink-Adapter zugewiesen werden, um eine Gruppe zu bilden. Eine Gruppe kann entweder den Datenverkehr zwischen dem physischen und dem virtuellen Netzwerk auf einige oder alle Netzwerkkarten der Gruppe aufteilen oder ein passives Failover im Falle einer Hardwarestörung oder eines Netzwerkausfalls bereitstellen.

Mit *VLANs* kann ein einzelnes physisches LAN-Segment weiter aufgeteilt werden, sodass Portgruppen derart voneinander isoliert werden, als befänden sie sich in unterschiedlichen physischen Segmenten. Der Standard ist 802.1Q.

Der *VMkernel-TCP/IP-Netzwerkstapel* unterstützt iSCSI, NFS und VMotion. Virtuelle Maschinen führen TCP/IP-Stapel ihrer eigenen Systeme aus und verbinden sich auf Ethernet-Ebene über virtuelle Switches mit dem VMkernel. Zwei neue Funktionen in ESX Server 3, iSCSI und NFS, werden in diesem Kapitel als *IP-Speicher* bezeichnet. IP-Speicher bezeichnet jedwede Art von Speicher, der auf TCP/IP-Netzwerkkommunikation beruht. iSCSI kann als Datenspeicher für virtuelle Maschinen verwendet werden. NFS kann als Datenspeicher für virtuelle Maschinen oder für die direkte Einbindung von `.ISO`-Dateien, die dann von der virtuellen Maschine als CD-ROMs erkannt werden, verwendet werden.

HINWEIS In den Netzwerkkapiteln wird beschrieben, wie das Netzwerk für iSCSI und NFS eingerichtet wird. Informationen zur Konfiguration des Speichers von iSCSI und NFS finden Sie in den Kapiteln zum Speicher.

TCP Segmentation Offload, *TSO*, ermöglicht einem TCP/IP-Stapel das Senden sehr großer Datenblöcke (bis zu 64 KB), obgleich die maximale Übertragungseinheit (Maximum Transmission Unit, MTU) der Schnittstelle kleiner ist. Der Netzwerkadapter trennt anschließend den großen Datenblock in Datenblöcke mit MTU-Größe und stellt eine angepasste Kopie der einleitenden TCP/IP-Header voran. Siehe „TCP-Segmentierungs-Offload und Jumbo-Frames“ auf Seite 65.

Über die *Migration mit VMotion* kann eine aktivierte virtuelle Maschine von einem ESX Server 3-Host auf einen anderen übertragen werden, ohne dass die virtuelle

Maschine heruntergefahren werden muss. Für die optionale VMotion-Funktion ist ein eigener Lizenzschlüssel notwendig.

Virtuelle Switches

Die VMware Infrastructure ermöglicht die Verwendung des Virtual Infrastructure (VI)-Clients oder Steuerung von SDK-APIs, um isolierte Netzwerkgeräte zu erstellen, die virtuelle Switches (vSwitches) genannt werden. Ein vSwitch kann Datenverkehr intern zwischen virtuellen Maschinen und zwischen virtuellen Maschinen und externen Netzwerken steuern.

HINWEIS Sie können auf einem einzelnen Host maximal 127 vSwitches einrichten.

Mit virtuellen Switches können Sie die Bandbreite mehrerer Netzwerkadapter kombinieren und den Datenverkehr darauf verteilen. Diese Switches können auch konfiguriert werden, um ein physisches Failover von Netzwerkkarten zu gewährleisten.

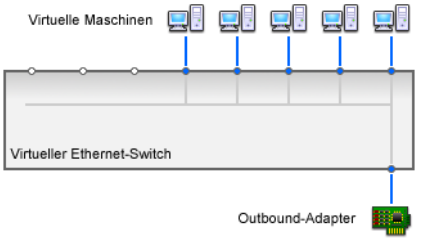
Ein vSwitch bildet einen physischen Ethernet-Switch ab. Die Standardanzahl der logischen Ports auf einem vSwitch ist 56. Mit ESX Server 3 können jedoch vSwitches mit bis zu 1016 Ports erstellt werden. An jeden dieser Ports können Sie einen Netzwerkadapter einer virtuellen Maschine anschließen. Jeder Uplink-Adapter, der mit einem vSwitch verknüpft wurde, verwendet einen Port. Jeder logische Port auf dem vSwitch gehört zu einer einzelnen Portgruppe. Jedem vSwitch kann darüber hinaus mindestens eine Portgruppe zugewiesen werden. Siehe „Portgruppen“ auf Seite 24.

Bevor der Netzwerkzugriff der virtuellen Maschinen konfiguriert werden kann, müssen die folgenden Aufgaben ausgeführt werden:

1. Einen vSwitch erstellen und diesen so konfigurieren, dass dieser mit den physischen Adaptern auf dem Host für das erforderliche physische Netzwerk verbunden wird.
2. Eine Portgruppe virtueller Maschinen erstellen, die mit diesem vSwitch verbunden wird, und ihr einen Namen geben, der von der Konfiguration der virtuellen Maschinen referenziert wird.

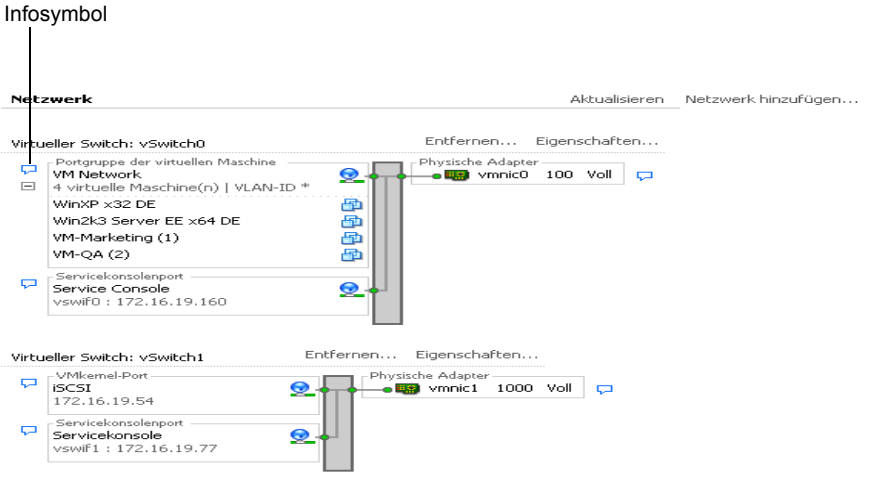
Wenn zwei oder mehr virtuelle Maschinen an den gleichen vSwitch angeschlossen sind, wird der Netzwerkdatenverkehr zwischen diesen virtuellen Maschinen lokal gesteuert. Wenn ein Uplink-Adapter dem vSwitch hinzugefügt ist, kann jede virtuelle Maschine auf das externe Netzwerk zugreifen, mit dem der Adapter verbunden ist (siehe Abbildung 2-1).

Abbildung 2-1. Verbindungen der virtuellen Switches



Im VI-Client werden die Einzelheiten des ausgewählten vSwitches als interaktives Diagramm dargestellt (siehe Abbildung 2-2). Die wichtigsten Informationen zu allen vSwitches werden stets angezeigt.

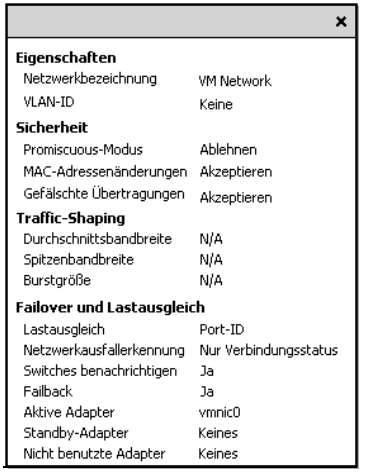
Abbildung 2-2. Interaktives Diagramm des virtuellen Switches



Klicken Sie auf das Infosymbol, um weitere detailliertere Informationen anzuzeigen.

Ein Popup-Fenster verweist auf die detaillierten Eigenschaften (siehe Abbildung 2-3).

Abbildung 2-3. Detaillierte Eigenschaften des virtuellen Switches



Portgruppen

Portgruppen vereinen mehrere Ports unter einer gemeinsamen Konfiguration und bieten so einen stabilen Ankerpunkt für virtuelle Maschinen, die an benannte Netzwerke angeschlossen sind. Jede Portgruppe wird durch eine Netzwerkbezeichnung gekennzeichnet, die für den aktuellen Host eindeutig ist.

HINWEIS Sie können auf einem einzelnen Host maximal 512 Portgruppen anlegen.

Eine VLAN-ID, die den Datenverkehr der Portgruppe auf ein logisches Ethernet-Segment im physischen Netzwerk einschränkt, kann optional zugewiesen werden.

HINWEIS Damit eine Portgruppe Portgruppen erreichen kann, die sich in anderen VLANs befinden, stellen Sie die VLAN-ID auf 4095 ein.

Aktivieren von Netzwerkdiensten

Bei ESX Server 3 müssen zwei Arten von Netzwerkdiensten aktiviert werden:

- Virtuelle Maschinen mit dem physischen Netzwerk verbinden
- VMkernel-Dienste (zum Beispiel NFS, iSCSI oder VMotion) mit dem physischen Netzwerk verbinden

Die Vernetzung der Servicekonsole, auf der die Verwaltungsdienste für ESX Server 3 ausgeführt werden, wird automatisch während der Installation eingerichtet. Ein Servicekonsolenport ist für ESX Server 3 erforderlich, damit eine Verbindung mit Netzwerk- oder Remotediensten, einschließlich VI-Client, eingerichtet werden kann. Für bestimmte Dienste, z. B. iSCSI-Speicher, sind ggf. weitere Servicekonsolenports erforderlich. Informationen zum Konfigurieren von Servicekonsolenports finden Sie unter „Konfiguration der Servicekonsole“ auf Seite 34.

Anzeigen der Netzwerkinformationen im VI-Client

Der VI-Client zeigt sowohl die allgemeinen Netzwerkinformationen als auch solche Informationen an, die spezifisch für Netzwerkadapter sind.

So zeigen Sie allgemeine Netzwerkinformationen auf dem VI-Client an

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.

Das Netzwerkfenster zeigt die folgenden Informationen an (siehe Abbildung 2-4):

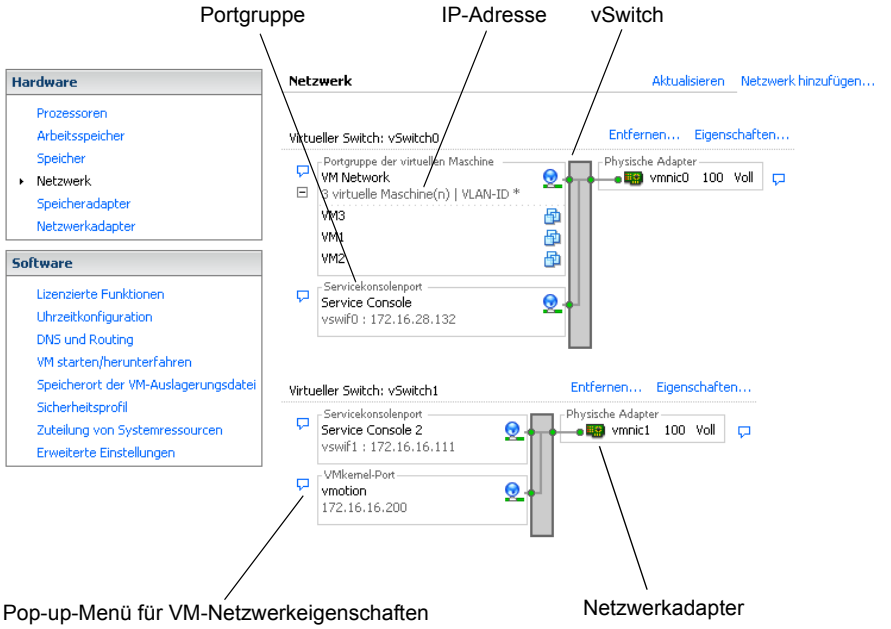
- Virtuelle Switches
- Adapterinformationen zu allen Adaptern
  - Verbindungsstatus
  - Nenngeschwindigkeit und Duplex
- Servicekonsolen- und VMkernel-TCP/IP-Dienste

  IP-Adresse
- Servicekonsole

  Name des virtuellen Geräts
- Virtuelle Maschinen
  - Betriebsstatus
  - Verbindungsstatus

- Portgruppe
  - Netzwerkbezeichnung – für alle drei Typen der Port-Konfiguration einheitlich
  - Anzahl der konfigurierten virtuellen Maschinen
  - VLAN-ID, falls vorhanden – für alle drei Typen der Port-Konfiguration einheitlich

Abbildung 2-4. Allgemeine Netzwerkinformationen



So zeigen Sie die Netzwerkadapterinformationen auf dem VI-Client an

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerkadapter (Network Adapters)**.

Das Netzwerkadapterfenster zeigt die folgenden Informationen an:

- **Gerät (Device)** – Name des Netzwerkadapters
- **Geschwindigkeit (Speed)** – Tatsächliche Geschwindigkeit und Duplex des Netzwerkadapters
- **Konfiguriert (Configured)** – Konfigurierte Geschwindigkeit und Duplex des Netzwerkadapters
- **vSwitch** – vSwitch, dem der Netzwerkadapter zugeordnet ist
- **Überwachte IP-Bereiche (Observed IP ranges)** – IP-Adressen, auf die der Netzwerkadapter zugreifen kann
- **Wake-on-LAN unterstützt (Wake on LAN supported)** – Fähigkeit des Netzwerkadapters zur Unterstützung von Wake-on-LAN

Konfiguration virtueller Netzwerke für virtuelle Maschinen

Der VI-Client-Assistent zum Hinzufügen von Netzwerken leitet Sie durch die Schritte zur Erstellung eines virtuellen Netzwerks, mit dem sich virtuelle Maschinen verbinden können. Zu diesen Aufgaben gehören u. a.:

- Einrichten des Verbindungstyps für eine virtuelle Maschine
- Hinzufügen eines virtuellen Netzwerks zu einem neuen oder einem bestehenden vSwitch
- Konfigurieren der Verbindungseinstellungen für die Netzwerkbezeichnung und die VLAN-ID

Weitere Informationen zum Konfigurieren von Netzwerkverbindungen für eine einzelne virtuelle Maschine finden Sie im *Basishandbuch für Systemadministratoren*.

Bedenken Sie beim Einrichten von Netzwerken mit virtuellen Maschinen, ob Sie die virtuellen Maschinen des Netzwerks zwischen ESX Server 3-Hosts migrieren möchten. Falls ja, stellen Sie sicher, dass sich beide Hosts in derselben Broadcast-Domäne befinden, also im selben Schicht 2-Subnetz.

ESX Server 3 unterstützt die Migration virtueller Maschinen zwischen Hosts unterschiedlicher Broadcast-Domänen deshalb nicht, weil eine migrierte virtuelle Maschine möglicherweise Systeme und Ressourcen benötigen könnte, auf die sie aufgrund der Verschiebung in ein separates Netzwerk keinen Zugriff mehr hätte. Selbst wenn Ihre Netzwerkkonfiguration als Hochverfügbarkeitsumgebung

eingerichtet ist oder intelligente Switches enthält, die in der Lage sind, dem Bedarf einer virtuellen Maschine auch in verschiedenen Netzwerken zu entsprechen, könnte es sein, dass es in der ARP-Tabelle (Address Resolution Protocol) zu Verzögerungen bei der Aktualisierung und der Wiederaufnahme des Netzwerkverkehrs der virtuellen Maschine kommt.

Virtuelle Maschinen greifen über Uplink-Adapter auf physische Netzwerke zu. Ein vSwitch kann nur dann Daten in externe Netzwerke übertragen, wenn mindestens ein Netzwerkadapter an den vSwitch angeschlossen ist. Wenn zwei oder mehr Adapter an einen vSwitch angeschlossen sind, werden sie transparent gruppiert.

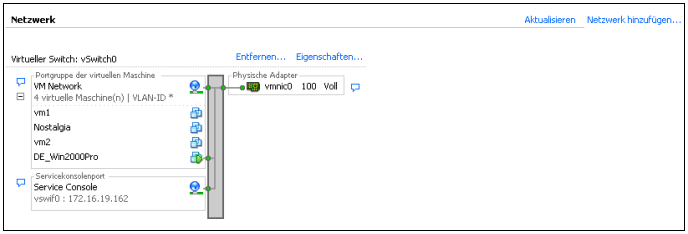
So erstellen Sie ein virtuelles Netzwerk für eine virtuelle Maschine

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.

Virtuelle Switches werden in einer Übersicht angezeigt, die ein detailliertes Layout enthält.



3 Klicken Sie auf der rechten Bildschirmseite auf **Netzwerk hinzufügen (Add Networking)**.

HINWEIS Der Assistent zum Hinzufügen von Netzwerken dient zum Hinzufügen neuer Ports und Portgruppen.

---

4 Akzeptieren Sie den Standardverbindungstyp **Virtuelle Maschinen (Virtual Machines)**.

Durch die Auswahl von **Virtuelle Maschinen (Virtual Machines)** können Sie ein benanntes Netzwerk hinzufügen, das den Datenverkehr im Netzwerk der virtuellen Maschinen verarbeitet.

5 Klicken Sie auf **Weiter (Next)**.

6 Klicken Sie auf **Virtuellen Switch erstellen (Create a virtual switch)**.

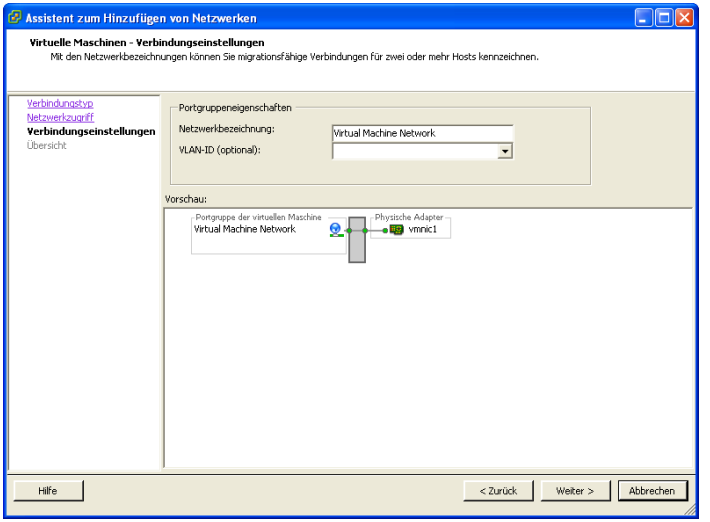
Sie können einen neuen vSwitch mit oder ohne Ethernet-Adapter erstellen.

Wenn Sie einen vSwitch ohne physische Netzwerkadapter erstellen, ist der Datenverkehr auf diesem vSwitch auf diesen vSwitch beschränkt. Andere Hosts im physischen Netzwerk oder virtuelle Maschinen auf anderen vSwitches können dann keine Daten über diesen vSwitch senden oder empfangen. Sie können einen vSwitch ohne physische Netzwerkadapter erstellen, wenn eine Gruppe virtueller Maschinen untereinander, nicht jedoch mit anderen Hosts oder virtuellen Maschinen außerhalb der Gruppe kommunizieren soll.

Änderungen werden im Bereich **Vorschau (Preview)** angezeigt.

7 Klicken Sie auf **Weiter (Next)**.

8 Geben Sie unter **Eigenschaften der Portgruppe (Port Group Properties)** eine Netzwerkbezeichnung für die zu erstellende Portgruppe ein.



Mit den Netzwerkbezeichnungen können Sie migrationsfähige Verbindungen für zwei oder mehr Hosts kennzeichnen.

9 Wenn Sie ein VLAN verwenden, geben Sie im Feld **VLAN-ID** eine Zahl zwischen 1 und 4094 ein.

Wenn Sie sich nicht sicher sind, was hier eingegeben werden muss, lassen Sie das Feld frei, oder wenden Sie sich an Ihren Netzwerkadministrator.

Wenn Sie 0 eingeben oder das Feld frei lassen, kann die Portgruppe nur nicht gekennzeichneten (Nicht-VLAN) Datenverkehr sehen. Wenn Sie 4095 eingeben,

kann die Portgruppe jeden Datenverkehr in einem VLAN sehen, und die VLAN-Kennzeichen bleiben intakt.

10 Klicken Sie auf **Weiter (Next)**.

11 Überprüfen Sie die ordnungsgemäße Konfiguration des vSwitches noch einmal, und klicken Sie dann auf **Fertig (Finish)**.

HINWEIS Verbinden Sie mindestens zwei Adapter mit einem Switch, um ein Failover (NIC-Gruppierung) zu aktivieren. Wenn ein Uplink-Adapter versagt, wird der Datenverkehr des Netzwerks auf einen anderen Adapter, der an den Switch angeschlossen ist, umgeleitet. Die NIC-Gruppierung erfordert, dass sich beide Ethernet-Geräte in derselben Ethernet-Broadcast-Domäne befinden.

Netzwerkkonfiguration des VMkernels

Die Verschiebung einer virtuellen Maschine von einem Host auf einen anderen wird Migration genannt. Die Migration einer aktivierten virtuellen Maschine wird als *VMotion* bezeichnet. Die Migration mit VMotion, die für den Einsatz zwischen hochkompatiblen Systemen entwickelt wurde, ermöglicht es Ihnen, virtuelle Maschinen ohne Ausfallzeiten zu migrieren. Der Protokollstapel des VMkernel muss ordnungsgemäß eingerichtet sein, damit VMotion funktioniert.

IP-Speicher bezeichnet jede Art von Speicher, die auf TCP/IP-Netzwerkkommunikation beruht. Dazu gehören iSCSI und NFS für ESX Server 3. Da diese beiden Speichertypen netzwerkbasiert sind, können beide die gleiche VMkernel-Schnittstelle und Portgruppe verwenden.

Die von VMkernel zur Verfügung gestellten Netzwerkdienste (iSCSI, NFS und VMotion) verwenden im VMkernel einen TCP/IP-Stapel. Dieser TCP/IP-Stapel ist vollständig vom TCP/IP-Stapel getrennt, der in der Servicekonsole verwendet wird. Jeder dieser TCP/IP-Stapel greift durch die Anbindung mindestens eines vSwitches an mindestens eine Portgruppe auf verschiedene Netzwerke zu.

TCP/IP-Stapel auf VMkernel-Ebene

Der TCP/IP-Netzwerkstapel von VMware VMkernel wurde erweitert und kann jetzt iSCSI, NFS und VMotion folgendermaßen verarbeiten:

- iSCSI als Datenspeicher für virtuelle Maschinen
- iSCSI zur direkten Einbindung von ISO-Dateien, die von virtuellen Maschinen als CD-ROMs erkannt werden
- NFS als Datenspeicher für virtuelle Maschinen
- NFS zur direkten Einbindung von `ISO`-Dateien, die von virtuellen Maschinen als CD-ROMs erkannt werden

- Migration mit VMotion

HINWEIS ESX Server 3 unterstützt über TCP/IP nur NFS, Version 3.

Aspekte und Richtlinien für die Konfiguration

Beachten Sie sich bei der Konfiguration des VMkernel-Netzwerks folgende Richtlinien:

- Die IP-Adresse, die Sie der Servicekonsole während der Installation zuweisen, darf nicht der IP-Adresse entsprechen, die Sie dem TCP/IP-Stapel des VMkernel auf der Registerkarte **Konfiguration (Configuration) > Netzwerk (Networking)** auf dem VMware Infrastructure-Client zugewiesen haben.
- Im Gegensatz zu anderen VMkernel-Diensten verfügt iSCSI über eine Servicekonsolenkomponente, sodass sowohl die Servicekonsole als auch VMkernel-TCP/IP-Stapel auf Netzwerke zugreifen können müssen, die zum Zugriff auf iSCSI-Ziele verwendet werden.
- Vor der Konfiguration von softwaregestütztem iSCSI für den ESX Server 3-Host muss ein Firewall-Port durch Aktivierung des iSCSI-Software-Client-Dienstes geöffnet werden. Siehe „Öffnen von Firewallports für unterstützte Dienste und Verwaltungs-Agenten“ auf Seite 198.

So richten Sie den VMkernel ein

1. Melden Sie sich am VMware VI-Client an und wählen Sie den Server in der Bestandsliste aus.

   Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2. Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.

3. Klicken Sie auf **Netzwerk hinzufügen (Add Networking)**.

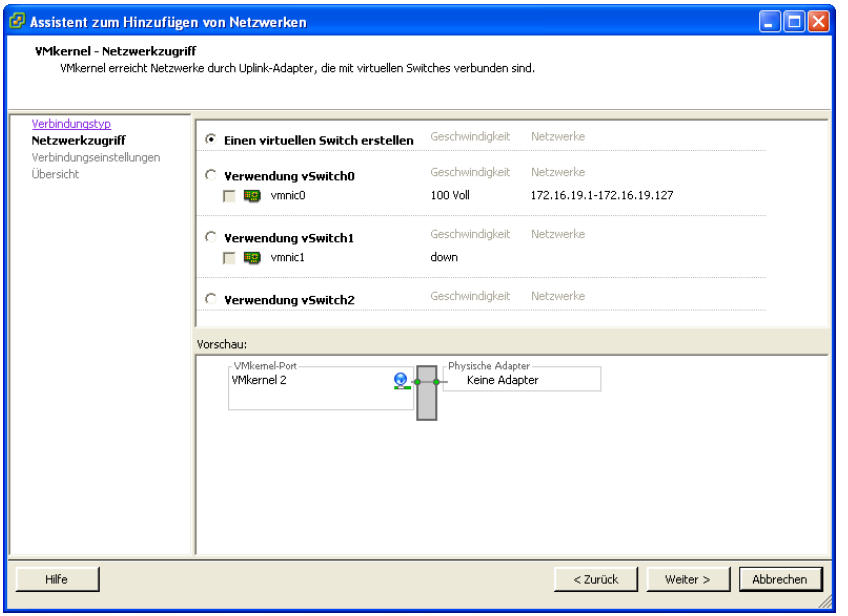
4. Wählen Sie **VMkernel** aus, und klicken Sie auf **Weiter (Next)**.

   Durch Auswahl der Option **VMotion und IP-Speicher (VMotion and IP Storage)** können Sie den VMkernel, der Dienste für VMotion und IP-Speicher (NFS oder iSCSI) ausführt, an ein physisches Netzwerk anschließen.

   Die Seite **Netzwerkzugriff (Network Access)** wird angezeigt.

5. Wählen Sie den vSwitch aus, den Sie verwenden möchten, oder aktivieren Sie **Einen virtuellen Switch erstellen (Create a virtual switch)**, um einen neuen vSwitch anzulegen.

6 Aktivieren Sie die Kontrollkästchen für die Netzwerkadapter, die Ihr vSwitch verwenden soll.



Die Auswahlmöglichkeiten werden im Bereich **Vorschau (Preview)** angezeigt.

Wählen Sie für jeden vSwitch Adapter aus, sodass die virtuellen Maschinen oder sonstigen Dienste, die an diesen Adapter angeschlossen sind, auf das richtige Ethernet-Segment zugreifen können. Wenn unter **Neuen virtuellen Switch erstellen (Create a new virtual switch)** keine Adapter angezeigt werden, bedeutet dies, dass alle Netzwerkadapter im System von vorhandenen vSwitches verwendet werden. Sie können entweder einen neuen vSwitch ohne Netzwerkadapter erstellen oder einen Netzwerkadapter auswählen, der von einem bereits vorhandenen vSwitch verwendet wird.

Weitere Informationen zum Verschieben von Netzwerkadaptern zwischen vSwitches finden Sie unter „So fügen Sie Uplink-Adapter hinzu“ auf Seite 45.

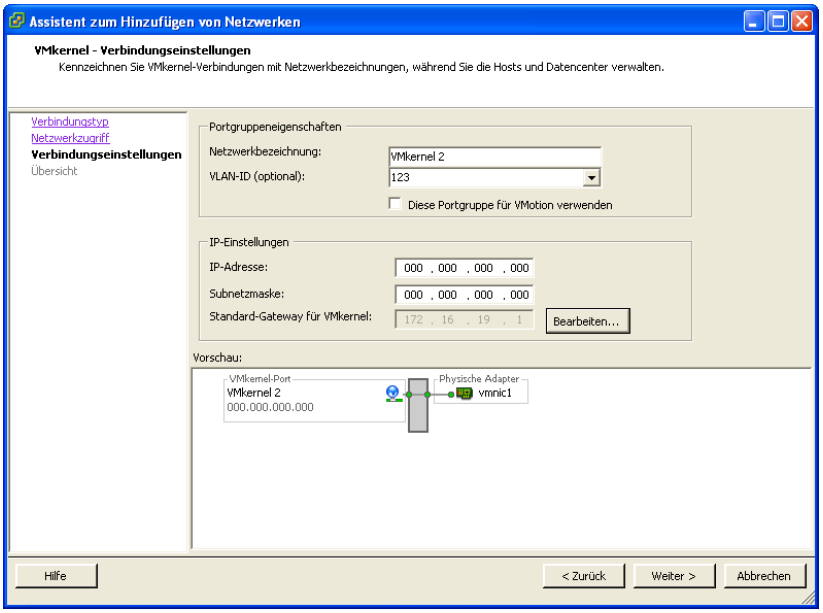
7 Klicken Sie auf **Weiter (Next)**.

8 Wählen Sie unter **Eigenschaften der Portgruppe (Port Group Properties)** eine Netzwerkbezeichnung und eine VLAN-ID aus bzw. geben Sie diese ein.

- **Netzwerkbezeichnung (Network Label)** – Ein Name, der die Portgruppe bezeichnet, die erstellt wird. Es handelt sich dabei um die Bezeichnung, die Sie bei der Konfiguration von VMkernel-Diensten wie VMotion und IP-Speicher während der Konfiguration des virtuellen Adapters, der an diese Portgruppe angeschlossen wird, festlegen.
- **VLAN-ID** – Kennzeichnet das VLAN, das für den Netzwerkdatenverkehr der Portgruppe verwendet wird.

9 Aktivieren Sie **Diese Portgruppe für VMotion verwenden (Use this port group for VMotion)**, damit diese Portgruppe anderen ESX-Servern melden kann, dass sie als Netzwerkverbindung dient, an die VMotion-Datenverkehr gesendet werden soll.

Auf jedem ESX Server 3-Host kann diese Eigenschaft nur für eine VMotion- und IP-Speicher-Portgruppe aktiviert werden. Wenn diese Eigenschaft für keine der Portgruppen aktiviert wurde, ist eine VMotion-Migration auf diesen Host nicht möglich.



10 Klicken Sie unter **IP-Einstellungen (IP Settings)** auf **Bearbeiten (Edit)**, um **Standard-Gateway für VMkernel (VMkernel Default Gateway)** für VMkernel-Dienste wie VMotion, NAS und iSCSI einzurichten.

HINWEIS Legen Sie ein Standard-Gateway für den Port fest, den Sie erstellt haben. VirtualCenter 2 verhält sich anders als VirtualCenter 1.x. Sie müssen eine gültige IP-Adresse und keine Pseudoadresse angeben, um den VMkernel-IP-Stapel zu konfigurieren.

Auf der Registerkarte **DNS-Konfiguration (DNS Configuration)** ist im Namensfeld standardmäßig der Hostname eingetragen. Auch die DNS-Server-Adressen und die Domäne, die während der Installation angegeben wurden, werden automatisch ausgefüllt.

Auf der Registerkarte **Routing** benötigen die Servicekonsole und der VMkernel jeweils eigene Gateway-Angaben. Ein Gateway ist zur Anbindung an Computer notwendig, die sich nicht im gleichen IP-Subnetz wie die Servicekonsole oder der VMkernel befinden.

Statische IP-Einstellungen sind voreingestellt.

11 Klicken Sie auf **OK** und dann auf **Weiter (Next)**.

12 Wenn Sie Änderungen vornehmen möchten, verwenden Sie die Schaltfläche **Zurück (Back)**.

13 Überprüfen Sie die Änderungen im Dialogfeld **Bereit zum Abschließen (Ready to Complete)**, und klicken Sie auf **Fertig (Finish)**.

Konfiguration der Servicekonsole

Die Servicekonsole und der VMkernel verwenden virtuelle Ethernet-Adapter zur Anbindung an einen vSwitch und zum Zugriff auf Netzwerke über diesen vSwitch.

Grundlegende Konfigurationsaufgaben für die Servicekonsole

Es gibt zwei übliche Konfigurationsänderungen für die Servicekonsole: Ändern von Netzwerkkarten (NICs) und von Einstellungen für eine vorhandene verwendete Netzwerkkarte.

Eine Änderung der Servicekonsolenkonfiguration ist nicht zulässig, wenn nur eine Servicekonsolenverbindung vorhanden ist. Wenn Sie eine neue Verbindung herstellen möchten, müssen Sie die Netzwerkeinstellungen so ändern, dass eine weitere Netzwerkkarte verwendet wird. Nach der Überprüfung der Funktionsfähigkeit der neuen Verbindung kann die alte Verbindung entfernt werden. Im Prinzip wechseln Sie also zu einer neuen Netzwerkkarte.

HINWEIS In ESX Server 3 können Sie maximal 16 Servicekonsolenports erstellen.

So konfigurieren Sie die Servicekonsole für den Netzwerkbetrieb

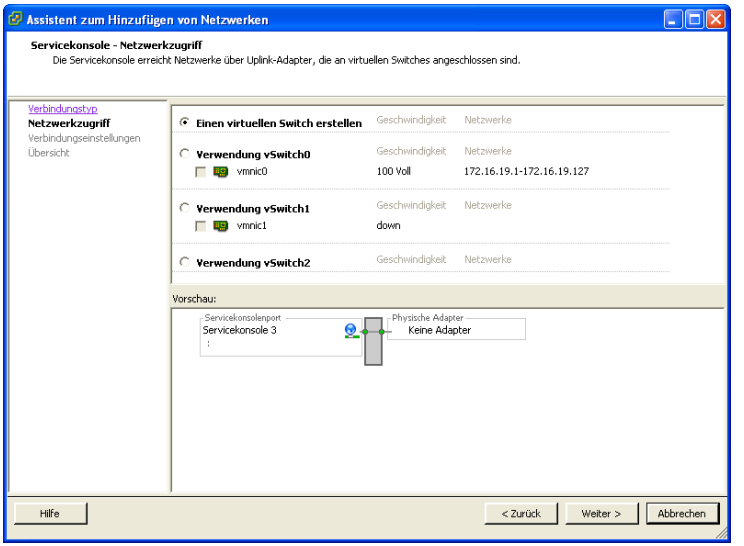
1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.

3 Klicken Sie auf **Netzwerk hinzufügen (Add Networking)**.

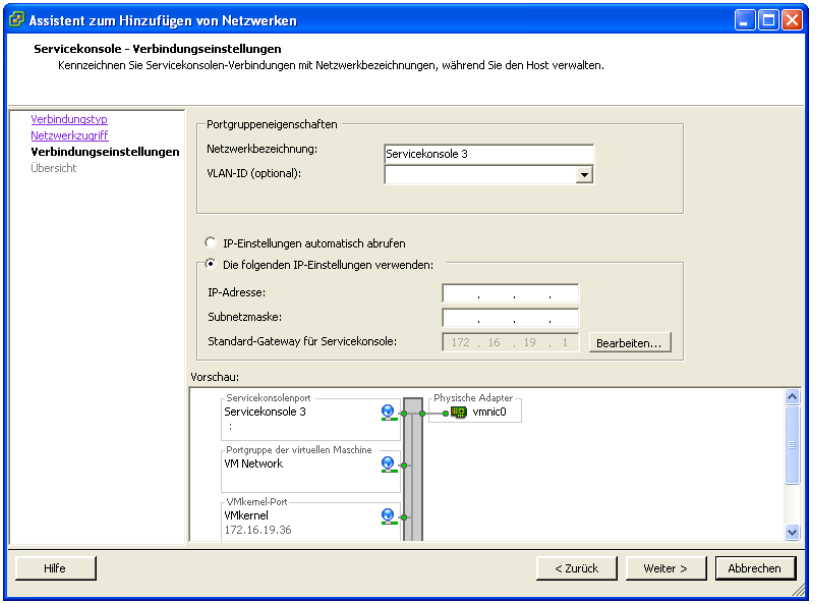
4 Wählen Sie im Dialogfeld **Verbindungstypen (Connection Types)** die Option **Servicekonsole (Service Console)** und klicken Sie auf **Weiter (Next)**.



5 Wählen Sie den vSwitch aus, den Sie für den Zugriff auf das Netzwerk verwenden möchten, oder markieren Sie **Neuen vSwitch erstellen (Create a new vSwitch)**. Klicken Sie auf **Weiter (Next)**.

Wenn unter **Neuen virtuellen Switch erstellen (Create a new virtual switch)** keine Adapter angezeigt werden, bedeutet dies, dass alle Netzwerkadapter im System von vorhandenen vSwitches verwendet werden. Weitere Informationen zum Verschieben von Netzwerkadaptern zwischen vSwitches finden Sie unter „So fügen Sie Uplink-Adapter hinzu“ auf Seite 45.

6 Wählen Sie unter **Portgruppen-Eigenschaften (Port Group Properties)** die Optionen **Netzwerkbezeichnung (Network Label)** und **VLAN-ID** aus, bzw. geben Sie diese ein.



Neuere Ports und Portgruppen werden im vSwitch-Diagramm oben angezeigt.

7 Geben Sie die **IP-Adresse (IP Address)** und die **Subnetzmaske (Subnet Mask)** ein, oder aktivieren Sie **IP-Einstellung automatisch beziehen (Obtain IP setting automatically)** für die IP-Adresse und die Subnetzmaske.

8 Klicken Sie auf die Schaltfläche **Bearbeiten (Edit)**, um **Standard-Gateway der Servicekonsole (Service Console Default Gateway)** festzulegen.

Siehe „So legen Sie das Standard-Gateway fest“ auf Seite 37.

9 Klicken Sie auf **Weiter (Next)**.

10 Überprüfen Sie die Angaben, und klicken Sie auf **Fertig (Finish)**.

So konfigurieren Sie Servicekonsolenports

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.

3 Suchen Sie rechts auf der Seite nach dem zu bearbeitenden vSwitch, und klicken Sie für diesen vSwitch auf **Eigenschaften (Properties)**.

4 Klicken Sie im Dialogfeld **vSwitch-Eigenschaften (vSwitch Properties)** auf die Registerkarte **Ports**.

5 Markieren Sie die Option **Servicekonsole (Service Console)**, und klicken Sie auf **Bearbeiten (Edit)**.

Es wird eine Warnmeldung angezeigt, dass möglicherweise durch Ändern der Servicekonsolenverbindung die Verbindungen für alle Verwaltungs-Agenten getrennt werden.

6 Klicken Sie auf **Änderung dieser Verbindung fortsetzen (Continue modifying this connection)**, um mit der Konfiguration der Servicekonsole fortzufahren.

7 Bearbeiten Sie die Porteigenschaften, die IP-Einstellungen und die geltenden Richtlinien, falls erforderlich.

8 Klicken Sie auf **OK**.

Pro TCP/IP-Stapel kann nur ein Standard-Gateway konfiguriert werden.

So legen Sie das Standard-Gateway fest

1 Melden Sie sich am VMware VI-Client an, und wählen Sie den Server aus der Bestandsliste aus.

Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **DNS und Routing (DNS and Routing)**.

Das Dialogfeld **DNS und Routing (DNS and Routing)** wird angezeigt.

3 Klicken Sie auf **Eigenschaften (Properties)**.

Auf der Registerkarte **DNS-Konfiguration (DNS Configuration)** ist im Namensfeld standardmäßig der Hostname eingetragen. Auch die DNS-Server-Adressen und die Domäne, die während der Installation angegeben wurden, werden automatisch eingetragen.

Auf der Registerkarte **Routing** sind die Servicekonsole und der VMkernel oft nicht an das gleiche Netzwerk angeschlossen und benötigen daher jeweils eigene Gateway-Daten. Ein Gateway wird zur Verbindung mit Computern benötigt, die sich nicht im selben IP-Subnetz wie die Servicekonsole oder der VMkernel befinden.

HINWEIS Alle NAS- und iSCSI-Server müssen entweder über das Standard-Gateway oder über dieselbe Broadcast-Domäne wie die zugeordneten vSwitches zu erreichen sein.

Bei der Servicekonsole ist ein Gateway nur notwendig, wenn mindestens zwei Netzwerkadapter dasselbe Subnetz verwenden. Das Gateway bestimmt, welcher Netzwerkadapter für die Standardroute verwendet wird.

4 Klicken Sie auf die Registerkarte **Routing**.

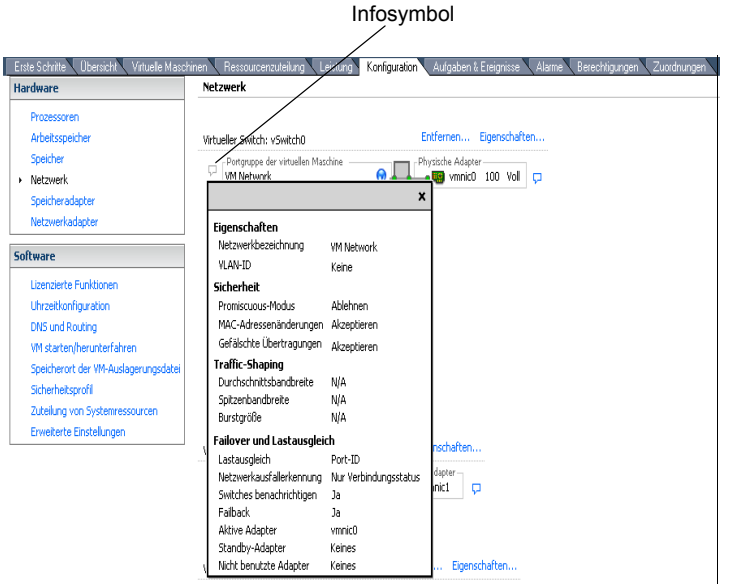
5 Stellen Sie das Standard-Gateway des VMkernels ein.

VORSICHT Es besteht das Risiko der Fehlkonfiguration, wodurch die Benutzeroberfläche die Anbindung an den Host verlieren kann. In diesem Fall muss der Host über die Befehlszeile der Servicekonsole neu konfiguriert werden. Vergewissern Sie sich, dass Ihre Netzwerkeinstellungen ordnungsgemäß sind, bevor Sie Änderungen speichern.

6 Klicken Sie auf **OK**.

So zeigen Sie Servicekonsoleninformationen an

1 Klicken Sie zur Anzeige von Servicekonsoleninformationen auf das Infosymbol.



2 Wenn Sie das Popup-Fenster schließen möchten, klicken Sie auf **X**.

Verwenden von DHCP für die Servicekonsole

In den meisten Fällen sollten für die Servicekonsole statische IP-Adressen verwendet werden. Wenn Ihr DNS-Server in der Lage ist, der dynamisch generierten IP-Adresse den Hostnamen der Servicekonsole zuzuordnen, können Sie für die Servicekonsole auch die dynamische IP-Adressierung (DHCP) verwenden.

Wenn der DNS-Server den Hostnamen nicht der dynamischen IP-Adresse zuweisen kann, müssen Sie die numerische IP-Adresse der Servicekonsole bestimmen und diese numerische IP-Adresse verwenden, wenn Sie auf den Host zugreifen.

Die numerische IP-Adresse kann sich ändern, wenn DHCP-Zuweisungen ablaufen oder das System neu gestartet wird. Aus diesem Grunde rät VMware davon ab, DHCP für die Servicekonsole zu verwenden, es sei denn, Ihr DNS-Server kann Hostnamen übersetzen.

Erweiterte Netzwerkthemen 3

Dieses Kapitel führt Sie durch die erweiterten Netzwerkthemen in einer ESX Server 3-Umgebung und durch die Einrichtung und Änderung erweiterter Netzwerkkonfigurationsoptionen.

In diesem Kapitel werden folgende Themen behandelt:

- „Eigenschaften und Richtlinien für virtuelle Switches“ auf Seite 42
- „Konfigurieren der Portgruppe“ auf Seite 60
- „DNS und Routing“ auf Seite 64
- „TCP-Segmentierungs-Offload und Jumbo-Frames“ auf Seite 65
- „NetQueue und Netzwerkleistung“ auf Seite 68
- „Einrichten von MAC-Adressen“ auf Seite 69
- „Optimale Vorgehensweisen und Tipps für Netzwerke“ auf Seite 71

Eigenschaften und Richtlinien für virtuelle Switches

In diesem Abschnitt werden die Konfiguration der Eigenschaften virtueller Switches und die Netzwerkrichtlinien behandelt, die auf der Ebene virtueller Switches konfiguriert werden.

Eigenschaften virtueller Switches

Die vSwitch-Einstellungen steuern Portstandardeinstellungen für den gesamten vSwitch, die durch Portgruppeneinstellungen für jeden Switch außer Kraft gesetzt werden können.

Bearbeiten der Eigenschaften virtueller Switches

Zur Bearbeitung der vSwitch-Eigenschaften gehört u. a.:

- die Konfiguration von Ports
- die Konfiguration der Uplink-Netzwerkadapter

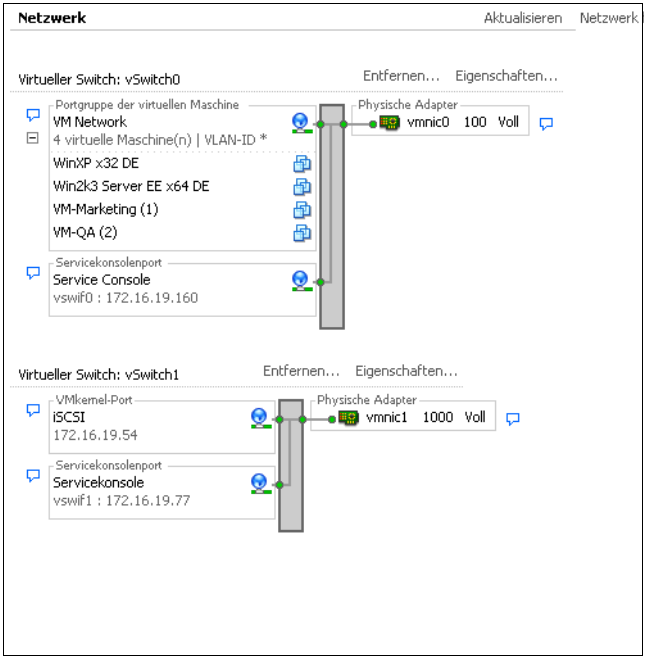
So bearbeiten Sie die Anzahl der Ports für einen vSwitch

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

   Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.

3 Suchen Sie auf der rechten Seite den vSwitch, den Sie bearbeiten möchten.



4 Klicken Sie auf **Eigenschaften (Properties)** für diesen vSwitch.

5 Klicken Sie auf die Registerkarte **Ports**.

6 Markieren Sie den vSwitch in der Liste **Konfiguration (Configuration)**, und klicken Sie auf **Bearbeiten (Edit)**.

7 Klicken Sie auf die Registerkarte **Allgemein (General)**, um die Anzahl der Ports festzulegen.

8 Wählen Sie die Anzahl der Ports, die Sie verwenden möchten, in der Dropdown-Liste aus.

9 Klicken Sie auf **OK**.

So konfigurieren Sie die Geschwindigkeit des Uplink-Netzwerkadapters

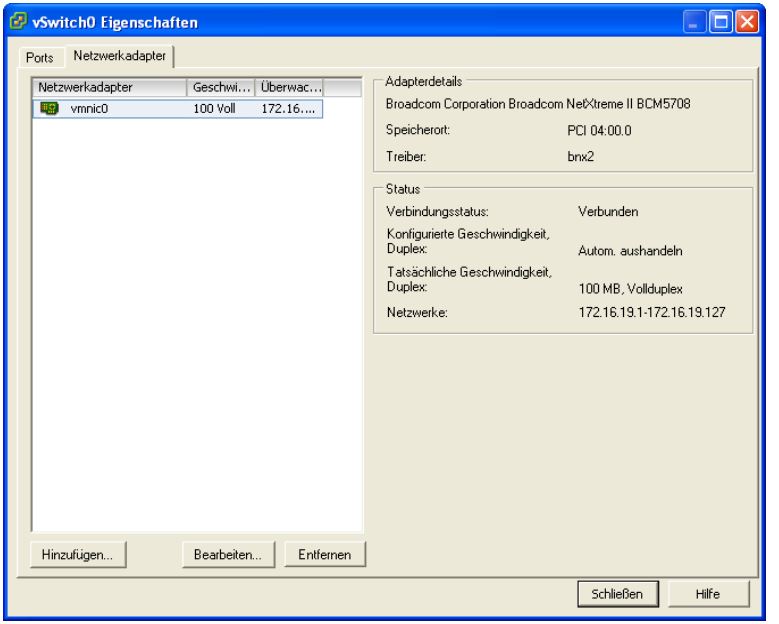
1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.

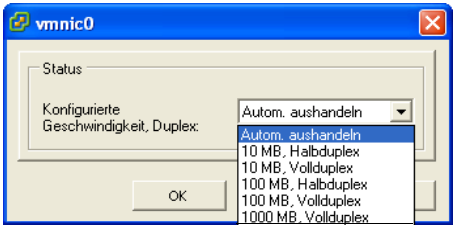
3 Wählen Sie einen vSwitch, und klicken Sie auf **Eigenschaften (Properties)**.

4 Klicken Sie auf die Registerkarte **Netzwerkadapter (Network Adapters)**.



5 Um die eingestellte Geschwindigkeit (den Duplexwert) eines Netzwerkadapters zu ändern, markieren Sie den Netzwerkadapter und klicken Sie auf **Bearbeiten (Edit)**.

Das Dialogfeld **Status** wird angezeigt. Die Standardeinstellung lautet **Autom. aushandeln (Autonegotiate)**, die meistens richtig ist.



6 Um die Verbindungsgeschwindigkeit manuell einzustellen, wählen Sie die Geschwindigkeits-/Duplexeinstellung im Dropdown-Menü aus.

Die Verbindungsgeschwindigkeit muss manuell eingestellt werden, wenn die Netzwerkkarte oder ein physischer Switch die ordnungsgemäße Verbindungsgeschwindigkeit nicht erkennen. Anzeichen für falsche Geschwindigkeits/Duplex-Einstellungen sind niedrige Bandbreite oder völlig fehlende Verbindung.

Der Adapter und der physische Switchport, an den der Adapter angeschlossen ist, müssen auf den gleichen Wert gesetzt werden, entweder Auto/Auto oder ND/ND (wobei ND für die Geschwindigkeit/Duplex steht), nicht jedoch Auto/ND.

7 Klicken Sie auf **OK**.

So fügen Sie Uplink-Adapter hinzu

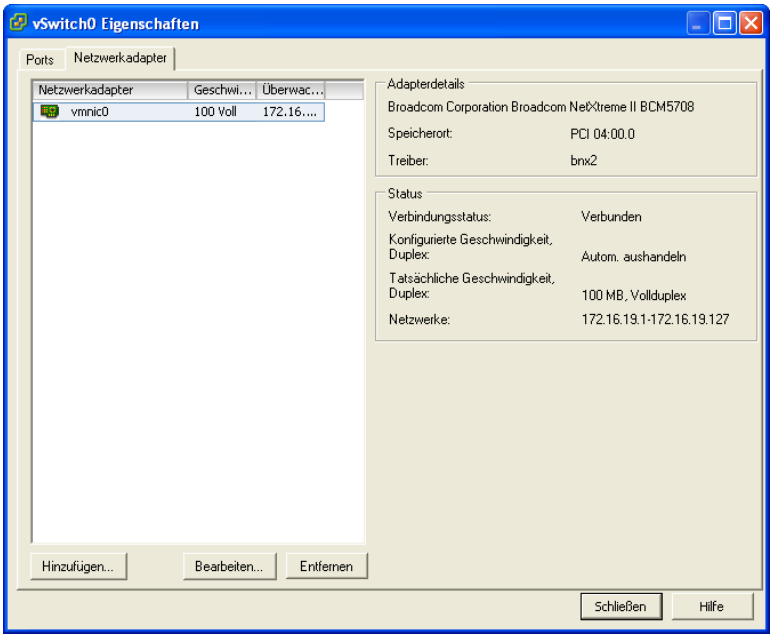
1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.

3 Wählen Sie einen vSwitch, und klicken Sie auf **Eigenschaften (Properties)**.

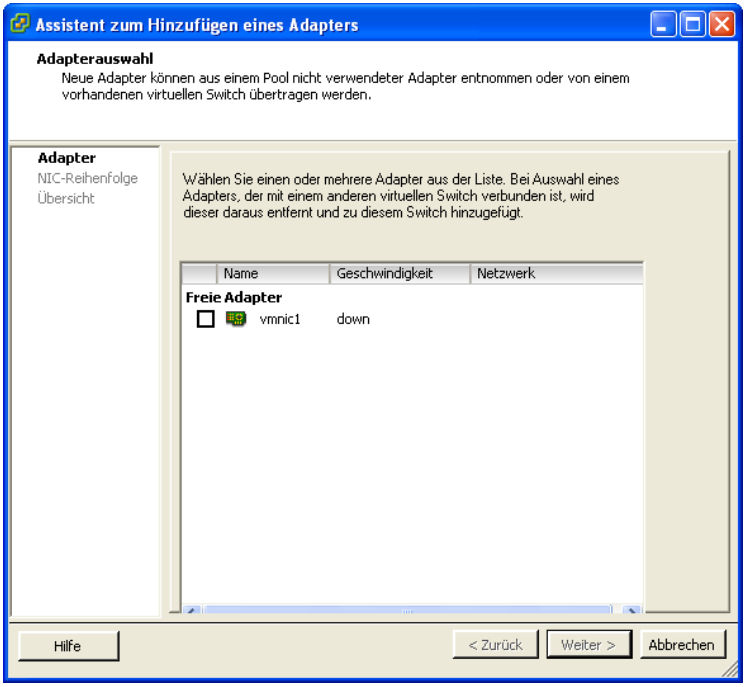
4 Klicken Sie im Dialogfeld **Eigenschaften (Properties)** auf die Registerkarte **Netzwerkadapter (Network Adapters)**.



5 Klicken Sie auf **Hinzufügen (Add)**. Der Assistent zum Hinzufügen eines Adapters wird aufgerufen.

Sie können einem einzelnen vSwitch mehrere Adapter zuweisen, um NIC-Gruppierung zu bewirken. Eine solche Gruppe kann den Datenverkehr gemeinsam verarbeiten und Ausfallsicherheit gewährleisten.

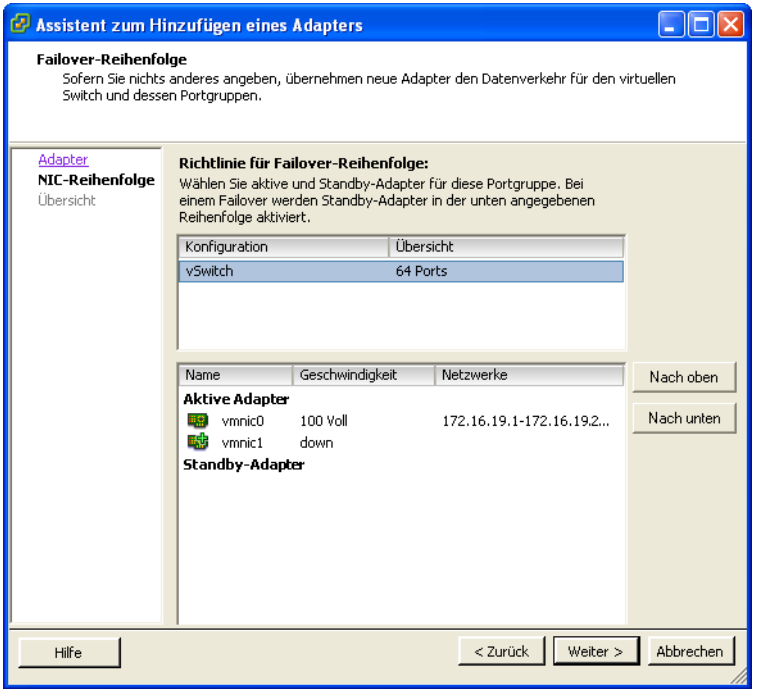
VORSICHT Eine Fehlkonfiguration kann dazu führen, dass der VI-Client nicht mehr auf den Host zugreifen kann.


Assistent zum Hinzufügen eines Adapters
Adapterauswahl
Neue Adapter können aus einem Pool nicht verwendeter Adapter entnommen oder von einem vorhandenen virtuellen Switch übertragen werden.
Adapter
NIC-Reihenfolge
Übersicht
Wählen Sie einen oder mehrere Adapter aus der Liste. Bei Auswahl eines Adapters, der mit einem anderen virtuellen Switch verbunden ist, wird dieser daraus entfernt und zu diesem Switch hinzugefügt.
Name
Geschwindigkeit
Netzwerk
Freie Adapter
vmnic1
down
Hilfe
< Zurück
Weiter >
Abbrechen

6 Wählen Sie mindestens einen Adapter in der Liste aus, und klicken Sie auf **Weiter (Next)**.

7 Sie können die Netzwerkkarten anordnen, indem Sie eine dieser Karten auswählen und auf die entsprechenden Schaltflächen klicken, um die Karte nach oben oder unten oder in eine andere Kategorie (**Aktiv (Active)** oder **Standby**) zu verschieben.

- **Aktive Adapter (Active Adapters)** – Adapter, die der vSwitch verwendet.
- **Standby-Adapter (Standby Adapters)** – Adapter, die aktiv werden, wenn einer oder mehrere der aktiven Adapter ausfallen.



8 Klicken Sie auf **Weiter (Next)**.

9 Überprüfen Sie die Informationen auf der Seite **Adapterübersicht (Adapter Summary)**, klicken Sie auf **Zurück (Back)**, wenn Sie Einträge ändern möchten, und klicken Sie schließlich auf **Fertig (Finish)**.

Die Liste der Netzwerkadapter mit den nun dem vSwitch zugewiesenen Adaptern wird erneut angezeigt.

10 Klicken Sie auf **Schließen (Close)**, um das Dialogfeld **vSwitch-Eigenschaften (vSwitch Properties)** zu schließen.

Der Abschnitt **Netzwerk (Networking)** auf der Registerkarte **Konfiguration (Configuration)** zeigt die Netzwerkadapter in ihrer festgelegten Reihenfolge und den gewählten Kategorien.

Cisco Discovery Protocol

Mit dem Cisco Discovery Protocol (CDP) können Administratoren von ESX Server 3 den Cisco-Switchport bestimmen, mit dem ein bestimmter vSwitch verbunden ist. Wenn CDP für einen bestimmten vSwitch aktiviert ist, können Sie im VI-Client Eigenschaften des Cisco-Switches anzeigen (z. B. Geräte-ID, Softwareversion und Zeitlimit).

Über die Befehlszeilenschnittstelle der Servicekonsole können Sie CDP aktivieren.

So aktivieren Sie CDP

1 Melden Sie sich direkt an der Konsole Ihres ESX Server 3-Hosts an.

2 Geben Sie den Befehl `esxcfg–vswitch –b <vSwitch>` ein, um den aktuellen CDP-Modus für den vSwitch anzuzeigen.

Ist CDP deaktiviert, wird der Modus als **down** angezeigt.

3 Geben Sie den Befehl `esxcfg–vswitch –B <mode> <vSwitch>` ein, um den CDP-Modus zu ändern.

Es folgen die möglichen CDP-Modi:

- **down** – CDP ist deaktiviert.
- **listen** – ESX Server 3 erkennt und zeigt Informationen zum verknüpften Cisco-Switchport an, die jedoch dem Administrator des Cisco-Switches nicht zur Verfügung stehen.
- **advertise** – ESX Server 3 stellt dem Cisco-Switch-Administrator Informationen zum vSwitch zur Verfügung, ohne jedoch Informationen zum Cisco-Switch zu erkennen bzw. anzuzeigen.
- **both** – ESX Server 3 erkennt und zeigt Informationen zum verknüpften Cisco-Switch an, die dem Administrator des Cisco-Switches zur Verfügung gestellt werden.

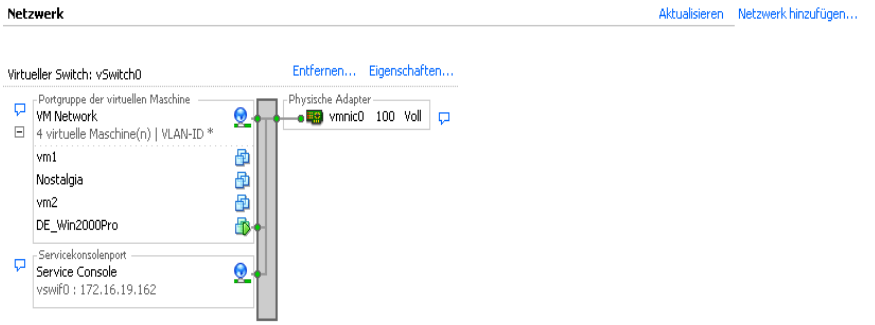
So zeigen Sie Cisco-Switchinformationen auf dem VI-Client an

1 Legen Sie den CDP-Modus für den vSwitch auf entweder **both** oder **listen** fest.

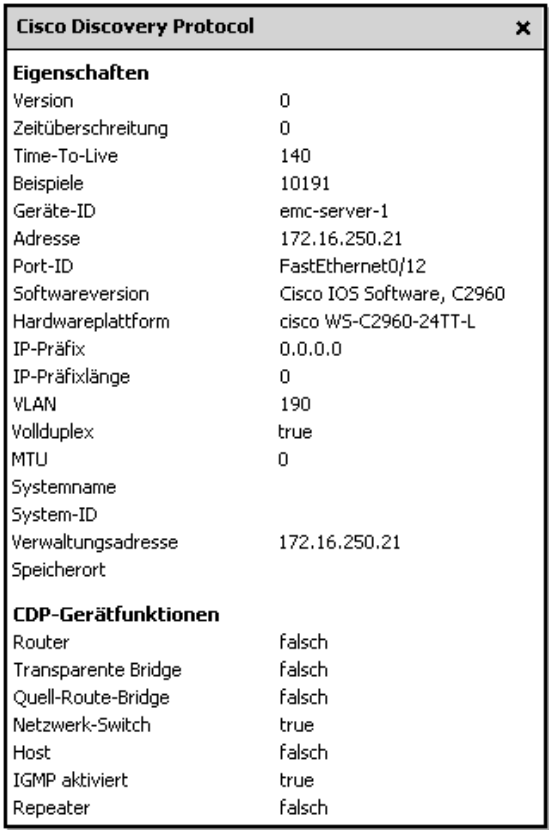
2 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

3 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.



4 Klicken Sie auf das Infosymbol rechts neben dem vSwitch.



Cisco Discovery Protocol

Eigenschaften	
Version	0
Zeitüberschreitung	0
Time-To-Live	140
Beispiele	10191
Geräte-ID	emc-server-1
Adresse	172.16.250.21
Port-ID	FastEthernet0/12
Softwareversion	Cisco IOS Software, C2960
Hardwareplattform	cisco WS-C2960-24TT-L
IP-Präfix	0.0.0.0
IP-Präfixlänge	0
VLAN	190
Vollduplex	true
MTU	0
Systemname	
System-ID	
Verwaltungsadresse	172.16.250.21
Speicherort	
CDP-Gerätfunktionen	
Router	falsch
Transparente Bridge	falsch
Quell-Route-Bridge	falsch
Netzwerk-Switch	true
Host	falsch
IGMP aktiviert	true
Repeater	falsch

HINWEIS Da die CDP-Hinweise zu Cisco-Geräten in der Regel einmal pro Minute generiert werden, kann es zwischen der Aktivierung von CDP für ESX Server 3 und der Verfügbarkeit von CDP-Daten auf dem VI-Client zu einer spürbaren Verzögerung kommen.

Richtlinien für virtuelle Switches

Sie können Richtlinien für den gesamten vSwitch festlegen, indem Sie den vSwitch oben auf der Registerkarte **Ports** auswählen und auf **Bearbeiten (Edit)** klicken.

Wenn Sie eine dieser Einstellungen für eine bestimmte Portgruppe außer Kraft setzen möchten, markieren Sie diese Portgruppe, und klicken Sie auf **Bearbeiten (Edit)**. Alle Änderungen der Einstellungen für den gesamten vSwitch werden auf alle Portgruppen auf diesem vSwitch angewendet. Ausgenommen hiervon sind die Konfigurationsoptionen, die von der Portgruppe außer Kraft gesetzt wurden.

Es gibt folgende Richtlinien für vSwitches:

- Schicht 2-Sicherheitsrichtlinie
- Traffic-Shaping-Richtlinie
- Richtlinie für Lastausgleich und Failover

Schicht 2-Sicherheitsrichtlinie

Schicht 2 ist die Sicherungsschicht. Die drei Elemente der Sicherheitsrichtlinie für Schicht 2 sind der Promiscuous-Modus, MAC-Adressenänderungen und gefälschte Übertragungen.

Im Nicht-Promiscuous-Modus überwacht der Gastadapter nur Datenverkehr an seiner eigenen MAC-Adresse. Im Promiscuous-Modus kann dieser alle Datenpakete überwachen. Per Voreinstellung ist Promiscuous-Modus für die Gastadapter deaktiviert.

Weitere Informationen zur Sicherheit finden Sie unter „Absichern der Ports virtueller Switches“ auf Seite 211.

So bearbeiten Sie die Sicherheitsrichtlinie für Schicht 2

1. Melden Sie sich am VMware VI-Client an, und wählen Sie den Server aus der Bestandsliste aus.

   Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

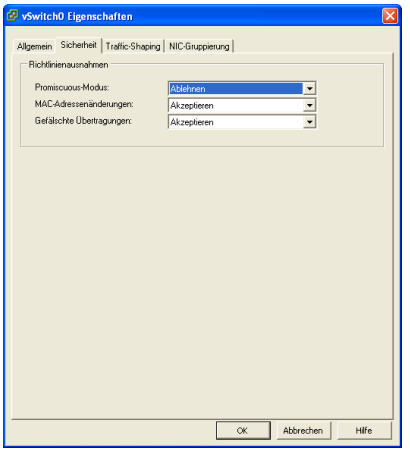
2. Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.

3. Klicken Sie für den vSwitch, dessen Schicht 2-Sicherheitsrichtlinie Sie bearbeiten möchten, auf **Eigenschaften (Properties)**.

4. Klicken Sie im Dialogfeld vSwitch-**Eigenschaften (Properties)** auf die Registerkarte **Ports**.

5. Wählen Sie das vSwitch-Element, und klicken Sie auf **Bearbeiten (Edit)**.

6 Klicken Sie im Dialogfeld Eigenschaften (Properties) des vSwitches auf die Registerkarte **Sicherheit (Security)**.



In der Standardeinstellung ist die Option **Promiscuous-Modus (Promiscuous Mode)** auf **Ablehnen (Reject)** festgelegt. **MAC-Adressenänderungen (MAC Address Changes)** und **Gefälschte Übertragungen (Forged Transmits)** sind auf **Akzeptieren (Accept)** eingestellt.

Diese Richtlinie gilt für alle virtuellen Adapter auf dem vSwitch, außer für diejenigen, für welche die Portgruppe für die virtuellen Adapter eine Ausnahme von der Richtlinie angibt.

7 Im Bereich **Richtlinienausnahmen (Policy Exceptions)** können Sie auswählen, ob die Ausnahmen für die Schicht 2-Sicherheitsrichtlinie abgelehnt oder angenommen werden sollen:

- **Promiscuous-Modus (Promiscuous Mode)**
  - **Ablehnen (Reject)** – Die Aktivierung des Promiscuous-Modus für den Gastadapter hat keine Auswirkungen darauf, welche Frames vom Adapter empfangen werden.
  - **Akzeptieren (Accept)** – Bei Aktivierung des Promiscuous-Modus für den Gastadapter werden alle Frames ermittelt, die über den vSwitch übertragen werden und die nach der VLAN-Richtlinie für die an den Adapter angeschlossene Portgruppe zugelassen sind.
- **MAC-Adressenänderungen (MAC Address Changes)**
  - **Ablehnen (Reject)** – Wenn die Option **MAC-Adressenänderungen (MAC Address Changes)** auf **Ablehnen (Reject)** festgelegt ist, und die MAC-Adresse des Adapters im Gastbetriebssystem in einen anderen Wert geändert wird als in den, der in der .vmx-Konfigurationsdatei angegeben ist, werden alle eingehenden Frames verworfen.

Wenn das Gastbetriebssystem die MAC-Adresse zurück in die MAC-Adresse in der .vmx-Konfigurationsdatei ändert, werden wieder alle eingehenden Frames durchgeleitet.

- **Akzeptieren (Accept)** – Die Änderung der MAC-Adresse des Gastbetriebssystems hat den gewünschten Effekt: Frames an die neue MAC-Adresse werden empfangen.

- **Gefälschte Übertragungen (Forged Transmits)**
  - **Ablehnen (Reject)** – Alle ausgehenden Frames, bei denen sich die MAC-Quelladresse von der für den Adapter festgelegten MAC-Adresse unterscheidet, werden verworfen.
  - **Akzeptieren (Accept)** – Es wird keine Filterung vorgenommen, und alle ausgehenden Frames werden durchgeleitet.

8 Klicken Sie auf **OK**.

Traffic-Shaping-Richtlinie

ESX Server 3 steuert den Datenverkehr durch die Festlegung von Parametern für drei Merkmale des ausgehenden Datenverkehrs: Durchschnittsbandbreite, Burstgröße und Spitzenbandbreite. Sie können die Werte für diese Merkmale über den VI-Client einstellen und somit die Traffic-Shaping-Richtlinie für jede Portgruppe festlegen.

- **Durchschnittsbandbreite (Average Bandwidth)** – Legt die zulässige Anzahl der Bits pro Sekunde fest, die den vSwitch im Durchschnitt durchlaufen darf, d. h. die zulässige durchschnittliche Datenlast.

- **Burstgröße (Burst Size)** legt die Höchstanzahl der Bytes fest, die in einem Burst zulässig sind. Wenn ein Burst den Burstgrößenparameter überschreitet, werden überzählige Datenpakete für eine spätere Übertragung zur Warteschlange hinzugefügt. Wenn die Warteschlange voll ist, werden die Pakete verworfen. Wenn Sie Werte für diese beiden Merkmale festlegen, geben Sie an, was der vSwitch während des Normalbetriebs voraussichtlich verarbeiten soll.

- Die **Spitzenbandbreite (Peak Bandwidth)** ist die höchste Bandbreite, die der vSwitch bieten kann, ohne Pakete verwerfen zu müssen. Wenn der Datenverkehr die festgelegte Spitzenbandbreite übersteigt, werden überzählige Pakete für eine spätere Übertragung zur Warteschlange hinzugefügt. Sobald der Datenverkehr wieder auf den Durchschnittswert zurückgegangen ist und ausreichende Kapazitäten zur Verfügung stehen, werden die Pakete in der Warteschlange verarbeitet. Wenn die Warteschlange voll ist, werden die Pakete verworfen. Selbst wenn Sie über Reservebandbreite verfügen, weil die Verbindung sich im Leerlauf befindet, beschränkt der Parameter „Spitzenbandbreite" die Übertragung auf den festgelegten Spitzenwert, bis der Datenverkehr zur zulässigen Durchschnittsdatenlast zurückkehrt.

So bearbeiten Sie die Traffic-Shaping-Richtlinie

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.

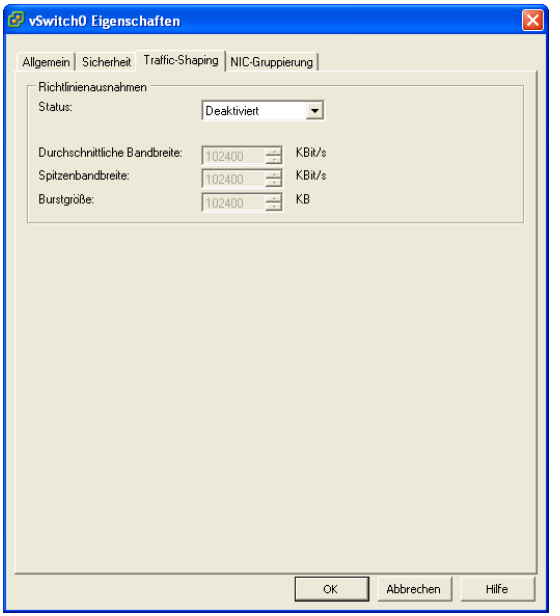
3 Wählen Sie einen vSwitch, und klicken Sie auf **Eigenschaften (Properties)**.

4 Klicken Sie im Dialogfeld **vSwitch-Eigenschaften (vSwitch Properties)** auf die Registerkarte **Ports**.

5 Wählen Sie den vSwitch, und klicken Sie auf **Bearbeiten (Edit)**.

6 Klicken Sie auf die Registerkarte **Traffic-Shaping (Traffic Shaping)**.

Wenn Traffic-Shaping deaktiviert ist, werden die einstellbaren Funktionen abgeblendet dargestellt. Sie können ausgewählte Traffic-Shaping-Funktionen auf Portgruppenebene außer Kraft setzen, wenn Traffic-Shaping aktiviert ist.



Diese Richtlinie wird in diesem Fall auf alle virtuellen Adapter angewendet, die an der Portgruppe angeschlossen sind, jedoch nicht auf den gesamten vSwitch.

Status – Wenn Sie die Richtlinienausnahmen im Feld **Status** aktivieren, begrenzen Sie die zugeteilte Netzwerkbandbreite für alle mit der betreffenden Portgruppe verknüpften virtuellen Adapter. Wenn Sie die Richtlinie deaktivieren, besteht für Dienste standardmäßig eine uneingeschränkte Verbindung zum physischen Netzwerk.

Die übrigen Felder legen die Parameter für den Netzwerkdatenverkehr fest:

- **Durchschnittsbandbreite (Average Bandwidth)** ist ein Wert, der über einen bestimmten Zeitraum gemessen wird.
- **Spitzenbandbreite (Peak Bandwidth)** ist ein Wert, der die zulässige Höchstbandbreite angibt und mindestens genauso groß wie die Durchschnittsbandbreite sein muss. Dieser Parameter schränkt die Höchstbandbreite während eines Bursts ein.
- **Burstgröße (Burst Size)** ist ein Wert, der angibt, wie groß ein Burst sein darf (in Kilobyte [KB]). Dieser Parameter steuert die Datenmenge, die während eines Bursts übertragen werden kann.

Richtlinie für Lastausgleich und Failover

Mit den Lastausgleichs- und Failover-Richtlinien können Sie festlegen, wie der Netzwerkdatenverkehr zwischen den Adaptern verteilt wird und wie der Verkehr neu geroutet wird, wenn ein Adapter ausfällt. Dazu müssen Sie die folgenden Parameter konfigurieren:

- Die **Lastausgleichsrichtlinie (Load Balancing policy)** legt fest, wie der ausgehende Datenverkehr über die Netzwerkadapter verteilt wird, die einem vSwitch zugewiesen wurden.

  HINWEIS Der eingehende Datenverkehr wird durch die Lastausgleichsrichtlinie auf dem physischen Switch gesteuert.

- **Failover-Erkennung (Failover Detection)**: Verbindungsstatus und Signalprüfung
- **Reihenfolge der Netzwerkadapter (Network Adapter Order)** (Aktiv/Standby)

So bearbeiten Sie die Richtlinie für Failover und Lastausgleich

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

  Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.

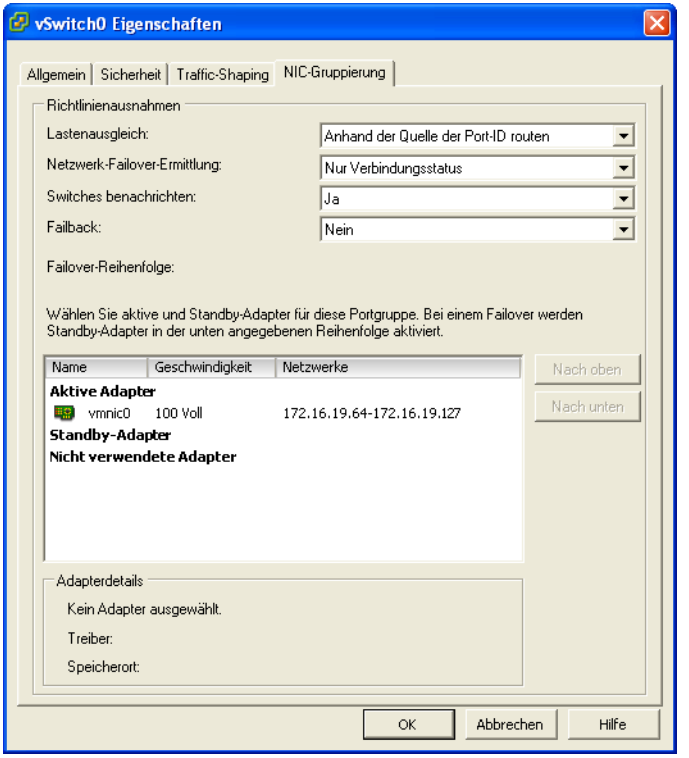
3 Wählen Sie einen vSwitch, und klicken Sie auf **Bearbeiten (Edit)**.

4 Klicken Sie im Dialogfeld **vSwitch-Eigenschaften (vSwitch Properties)** auf die Registerkarte **Ports**.

5 Markieren Sie den vSwitch und klicken Sie auf **Eigenschaften (Properties)**, um die Werte für **Failover und Lastausgleich (Failover and Load Balancing)** für den vSwitch zu bearbeiten.

6 Klicken Sie auf die Registerkarte **NIC-Gruppierung (NIC Teaming)**.

Sie können die Failover-Reihenfolge auf Portgruppenebene außer Kraft setzen. Standardmäßig werden neue Adapter für alle Richtlinien aktiviert. Neue Adapter übertragen den Datenverkehr für den vSwitch und seine Portgruppe, wenn Sie nichts anderes angeben.



7 Unter **Richtlinienausnahmen (Policy Exceptions)**:

- **Lastausgleich (Load Balancing)** – Geben Sie an, wie ein Uplink ausgewählt werden soll.
  - **Anhand der Quelle der Port-ID routen (Route based on the originating port ID)** – Der Uplink wird anhand des virtuellen Ports ausgewählt, an dem der Datenverkehr den virtuellen Switch ansteuert.
  - **Anhand des IP-Hashs routen (Route based on ip hash)** – Der Uplink wird anhand eines Hashs der Quell- und Ziel-IP-Adresse jedes Pakets ausgewählt. Bei Nicht-IP-Paketen wird zur Berechnung des Hashs der Wert verwendet, der im Offset eingetragen ist.
  - **Anhand des Quell-MAC-Hashs routen (Route based on source MAC hash)** – Der Uplink wird anhand eines Hashs des Quell-Ethernets ausgewählt.
  - **Explizite Failover-Reihenfolge verwenden (Use explicit failover order)** – Es wird immer der Uplink ausgewählt, der an erster Stelle der Liste der aktiven Adapter steht und die Failover-Erkennungskriterien erfüllt.

HINWEIS Für eine IP-basierte Gruppierung ist es erforderlich, dass der physische Switch mit „etherchannel“ konfiguriert wird. Bei allen anderen Optionen muss „etherchannel“ deaktiviert sein.

- **Netzwerk-Failover-Erkennung (Network Failover Detection)** – Geben Sie die Verfahrensweise zur Verwendung der Failover-Erkennung an.
  - **Nur Verbindungsstatus (Link Status only)** – Als Grundlage dient ausschließlich der vom Netzwerkadapter angegebene Verbindungsstatus. Über diese Option werden Fehler wie nicht angeschlossene Kabel oder Betriebsausfälle des physischen Switches ermittelt, nicht jedoch Konfigurationsfehler, z. B. die Blockierung eines Ports des physischen Switches durch STP (Spanning Tree Protocol), eine Zuweisung zum falschen VLAN oder nicht angeschlossene Kabel an der anderen Seite eines physischen Switches.
  - **Signalprüfung (Beacon Probing)** – Sendet Signale, sucht nach Signalprüfpaketen auf allen Netzwerkkarten in der Gruppe und verwendet diese Informationen zusätzlich zum Verbindungsstatus, um einen Verbindungsausfall zu ermitteln. Dadurch können viele der zuvor genannten Ausfälle erkannt werden, die durch den Verbindungsstatus allein nicht erkannt werden können.

- **Switches benachrichtigen (Notify Switches)** – Wählen Sie **Ja (Yes)** oder **Nein (No)**, um Switches bei einem Failover zu benachrichtigen.

  Wenn Sie **Ja (Yes)** wählen, wird jedes Mal, wenn eine virtuelle Netzwerkkarte an einen virtuellen Switch angeschlossen wird, oder ein Failover-Ereignis dazu führt, dass der Datenverkehr einer virtuellen Netzwerkkarte über eine andere physische Netzwerkkarte geleitet wird, über das Netzwerk eine Meldung gesendet, um die Verweistabelle auf physischen Switches zu aktualisieren. In fast allen Fällen ist dies wünschenswert, um die Wartezeiten für Failover-Ereignisse und Migrationen mit VMotion zu minimieren.

  HINWEIS Verwenden Sie diese Option nicht, wenn die an die Portgruppe angeschlossenen virtuellen Maschinen den Netzwerklastausgleich (NLB) von Microsoft im Unicast-Modus verwenden. Im Multicast-Modus mit NLB treten keine Probleme auf.

- **Failback** – Wählen Sie **Ja (Yes)** oder **Nein (No)**, um Failback zu deaktivieren oder zu aktivieren.

  Diese Option bestimmt, wie ein physischer Adapter nach einem Ausfall wieder in den aktiven Betrieb genommen wird. Wenn die Option auf **Nein (No)** gesetzt wurde, wird der Adapter sofort nach der Wiederherstellung seiner Funktionsfähigkeit aktiviert. Er ersetzt in diesem Fall den ggf. vorhandenen Ersatzadapter, der seinen Platz eingenommen hatte. Wenn diese Option auf **Ja (Yes)** gesetzt wurde, bleibt ein ausgefallener Adapter nach der Wiederherstellung seiner Funktionsfähigkeit deaktiviert, bis der gegenwärtig aktive Adapter ausfällt und ersetzt werden muss.

- **Failover-Reihenfolge (Failover Order)** – Geben Sie an, wie die Verarbeitungslast für die Adapter verteilt werden soll. Wenn Sie bestimmte Adapter verwenden und andere für Notfälle reservieren möchten, sollten die verwendeten Adapter ausfallen, können Sie Adapter mithilfe des Dropdown-Menüs in zwei Gruppen aufteilen:

  - **Aktive Adapter (Active Adapters)** – Dieser Adapter wird weiter verwendet, wenn die Netzwerkadapterverbindung hergestellt und aktiv ist.
  - **Standby-Adapter (Standby Adapters)** – Dieser Adapter wird verwendet, wenn mindestens eine Verbindung des aktiven Adapters nicht verfügbar ist.
  - **Nicht verwendete Adapter (Unused Adapters)** – Dieser Adapter soll nicht verwendet werden.

Konfigurieren der Portgruppe

Sie können die folgenden Portgruppeneinstellungen ändern:

- Portgruppeneigenschaften
- Benannte Netzwerkrichtlinien

So bearbeiten Sie die Eigenschaften von Portgruppen

1. Melden Sie sich am VMware VI-Client an und wählen Sie den Server aus dem Bestandslistenfenster aus.

   Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2. Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.

3. Klicken Sie auf der rechten Seite des Fensters für ein Netzwerk auf **Eigenschaften (Properties)**.

4. Klicken Sie auf die Registerkarte **Ports**.

5. Wählen Sie die Portgruppe, und klicken Sie auf **Bearbeiten (Edit)**.

6. Klicken Sie im Dialogfeld **Eigenschaften (Properties)** der Portgruppe auf die Registerkarte **Allgemein (General)**, um folgende Einstellungen zu ändern:

   - **Netzwerkbezeichnung (Network Label)** – Bezeichnet die Portgruppe, die erstellt wird. Geben Sie diese Bezeichnung ein, wenn Sie einen virtuellen Adapter dieser Portgruppe zuweisen, entweder bei der Konfiguration von virtuellen Maschinen oder von VMkernel-Diensten, z. B. VMotion oder IP-Speicher.
   - **VLAN-ID** – Kennzeichnet das VLAN, das für den Netzwerkdatenverkehr der Portgruppe verwendet wird.

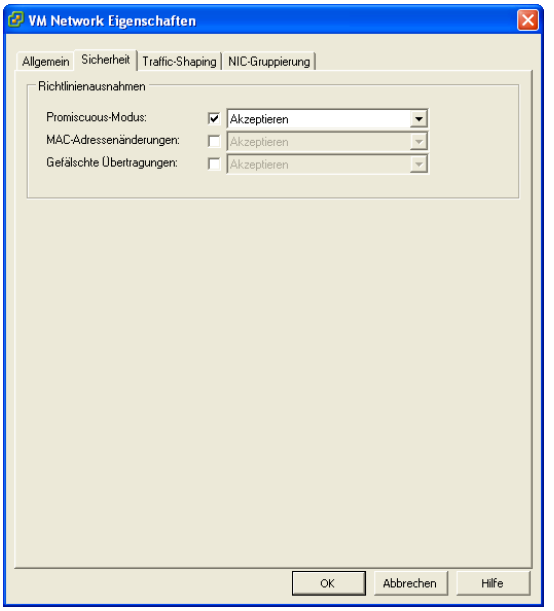
7. Klicken Sie auf **OK**.

So setzen Sie Richtlinien für bezeichnete Netzwerke außer Kraft

1 Um die Netzwerkrichtlinien eines bestimmten bezeichneten Netzwerks außer Kraft zu setzen, wählen Sie das Netzwerk aus, klicken Sie auf **Bearbeiten (Edit)** und anschließend auf die Registerkarte **Sicherheit (Security)**.

2 Aktivieren Sie das Kontrollkästchen für das bezeichnete Netzwerk, das Sie außer Kraft setzen möchten.

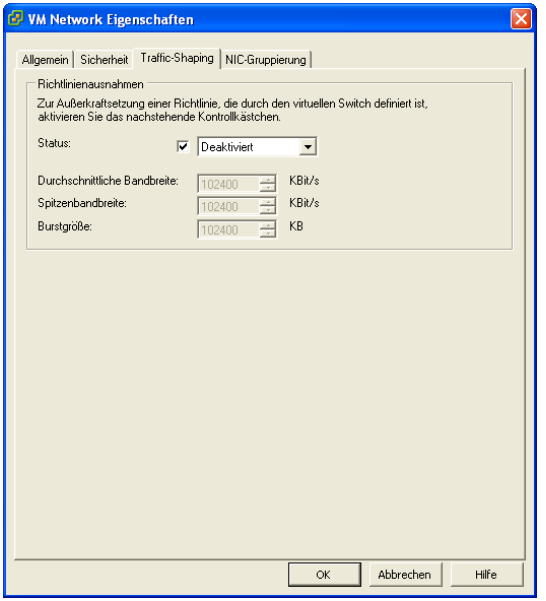
Weitere Informationen zu diesen Einstellungen finden Sie unter „Schicht 2-Sicherheitsrichtlinie“ auf Seite 52.



3 Klicken Sie auf die Registerkarte **Traffic-Shaping (Traffic Shaping).**

4 Aktivieren Sie das Kontrollkästchen neben **Status**, und wählen Sie **Aktiviert (Enabled)** oder **Deaktiviert (Disabled)** aus.

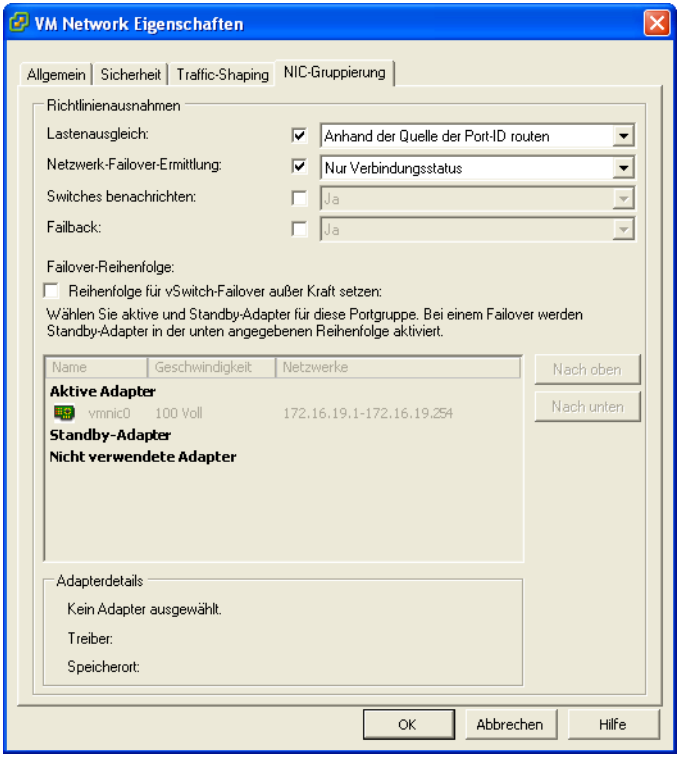
Weitere Informationen zu den Statuseinstellungen finden Sie unter „Traffic-Shaping-Richtlinie“ auf Seite 54.



5 Klicken Sie auf die Registerkarte **NIC-Gruppierung (NIC Teaming)**.

6 AktivierenSie das entsprechende Kontrollkästchen, um die Richtlinien für den Lastausgleich oder die Failover-Reihenfolge außer Kraft zu setzen.

Weitere Informationen zu diesen Einstellungen finden Sie unter „Richtlinie für Lastausgleich und Failover“ auf Seite 56.



7 Klicken Sie auf **OK**.

DNS und Routing

Konfigurieren Sie DNS und Routing über den VI-Client.

So ändern Sie die DNS- und Routing-Konfiguration

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **DNS und Routing (DNS and Routing)**.

3 Klicken Sie auf der rechten Bildschirmseite auf **Eigenschaften (Properties)**.

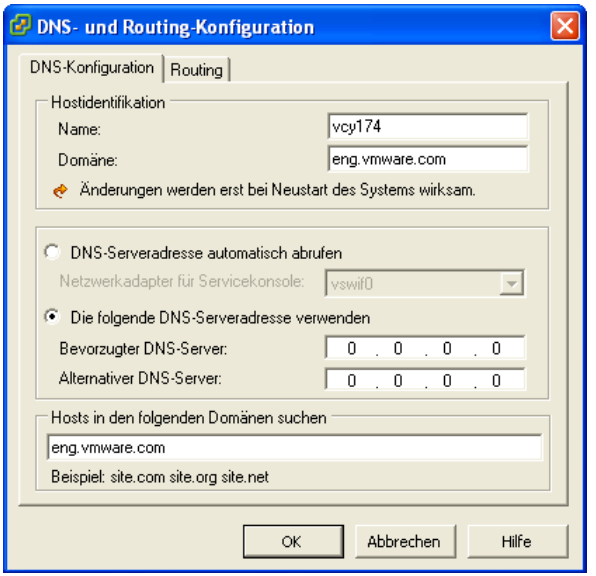
4 Geben Sie auf der Registerkarte **DNS-Konfiguration (DNS Configuration)** die Werte für **Name** und **Domäne (Domain)** ein.

5 Sie können die Adresse des DNS-Servers automatisch beziehen oder eine DNS-Server-Adresse eingeben.

HINWEIS DHCP wird nur unterstützt, wenn die Servicekonsole auf den DHCP-Server zugreifen kann. Für die Servicekonsole muss dazu eine virtuelle Schnittstelle (vswif) konfiguriert und an das Netzwerk angeschlossen werden, in dem sich der DHCP-Server befindet.

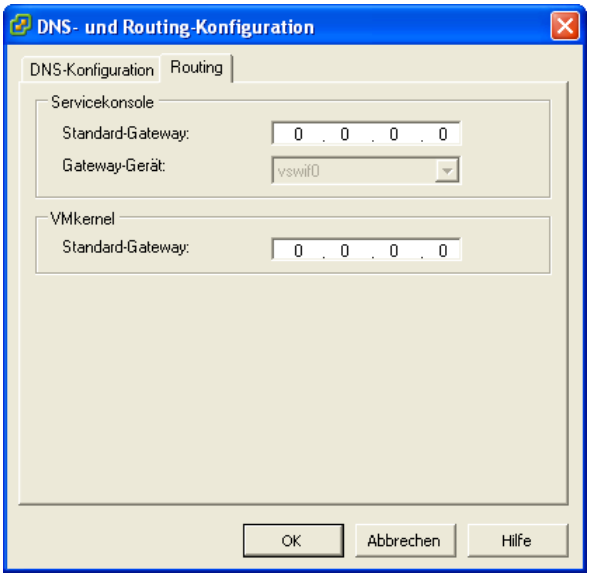
---

6 Geben Sie die Domänen an, in denen Hosts gesucht werden sollen.



7 Ändern Sie auf der Registerkarte **Routing** die Informationen zum Standard-Gateway nach Bedarf.

Wählen Sie ein Gateway-Gerät nur dann aus, wenn die Servicekonsole auf mehr als ein Subnetz zugreifen soll.



8 Klicken Sie auf **OK**.

TCP-Segmentierungs-Offload und Jumbo-Frames

Unterstützung für TCP Segmentation Offload (TSO) und Jumbo-Frames wurden dem TCP/IP-Stapel in ESX Server 3, Version 3.5, hinzugefügt. Jumbo-Frames müssen auf Serverebene über die Befehlszeilenschnittstelle aktiviert werden, indem die MTU-Größe für jeden vSwitch konfiguriert wird. TSO ist für die VMkernel-Schnittstelle standardmäßig aktiviert, muss jedoch auf virtueller Maschinenebene aktiviert werden.

Aktivieren von TSO

TSO-Unterstützung über den Netzwerkadapter „VMXnet (erweitert)" steht für virtuelle Maschinen mit den folgenden Gastbetriebssystemen zur Verfügung:

- Microsoft Windows 2003 Enterprise Edition mit Service Pack 2 (32-Bit und 64-Bit)
- Red Hat Enterprise Linux 4 (64-Bit)

- Red Hat Enterprise Linux 5 (32-Bit und 64-Bit)
- SuSE Linux Enterprise Server 10 (32-Bit und 64-Bit)

Um TSO auf virtueller Maschinenebene zu aktivieren, müssen Sie vorhandene virtuelle Netzwerkadapter vom Typ „vmxnet" oder „Flexibel" durch Netzwerkadapter vom Typ „VMXnet (erweitert)" ersetzen. Dadurch kann sich die MAC-Adresse des virtuellen Netzwerkadapters ändern.

So aktivieren Sie die TSO-Unterstützung für eine virtuelle Maschine

1 Melden Sie sich am VI-Client an, und wählen Sie die virtuelle Maschine in der Bestandsliste aus.

   Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf der Registerkarte **Übersicht (Summary)** auf **Einstellungen bearbeiten (Edit Settings)**.

3 Wählen Sie in der Liste **Hardware** den Netzwerkadapter aus.

4 Notieren Sie sich die Netzwerkeinstellungen und die MAC-Adresse des Netzwerkadapters.

5 Klicken Sie auf **Entfernen (Remove)**, um den Netzwerkadapter aus der virtuellen Maschine zu entfernen.

6 Klicken Sie auf **Hinzufügen (Add)**.

7 Wählen Sie **Ethernet-Adapter (Ethernet Adapter)**, und klicken Sie auf **Weiter (Next)**.

8 Wählen Sie unter **Adaptertyp (Adapter Type)** die Option **Vmxnet (erweitert) (Enhanced vmxnet)** aus.

9 Wählen Sie die Netzwerkeinstellungen und MAC-Adresse des alten Netzwerkadapters aus, und klicken Sie auf **Weiter (Next)**.

10 Klicken Sie auf **Fertig (Finish)**.

11 Klicken Sie auf **OK**.

12 Wenn die virtuelle Maschine nicht auf die Aktualisierung von VMware Tools bei jeder Aktivierung eingestellt ist, müssen Sie VMware Tools manuell aktualisieren. Siehe das *Basishandbuch für Systemadministratoren*.

Für eine VMkernel-Schnittstelle ist TSO standardmäßig aktiviert. Wenn TSO für eine bestimmte VMkernel-Schnittstelle deaktiviert sein sollte, besteht die einzige Möglichkeit zur Aktivierung von TSO im Löschen dieser VMkernel-Schnittstelle und ihrer erneuten Erstellung mit aktivierter TSO.

So prüfen Sie, ob TSO für eine VMkernel-Schnittstelle aktiviert ist

1 Melden Sie sich direkt an der Konsole Ihres ESX Server 3-Hosts an.

2 Geben Sie den Befehl `esxcfg-vmknic -l` ein, um eine Liste der VMkernel-Schnittstellen einzublenden

Jede für TSO aktivierte VMkernel-Schnittstelle muss in der Liste mit **TSO MSS** auf 40960 eingestellt angezeigt werden.

Wenn TSO für eine bestimmte VMkernel-Schnittstelle nicht aktiviert ist, besteht die einzige Möglichkeit zur Aktivierung von TSO im Löschen dieser VMkernel-Schnittstelle und ihrer erneuten Erstellung. Siehe „Netzwerkkonfiguration des VMkernels“ auf Seite 30.

Aktivieren von Jumbo-Frames

Mithilfe von Jumbo-Frames kann ESX Server 3 größere Frames an das physische Netzwerk senden. Das Netzwerk muss Jumbo-Frames durchgängig unterstützen, damit diese Technologie eingesetzt werden kann. Jumbo-Frames bis zu 9 KB (9000 Bytes) werden unterstützt. iSCSI mit Jumbo-Frames wird nicht unterstützt.

Jumbo-Frames muss über die Befehlszeilenschnittstelle Ihres ESX Server 3-Hosts für jede vSwitch- bzw. VMkernel-Schnittstelle aktiviert werden. Prüfen Sie vor der Aktivierung von Jumbo-Frames bei Ihrem Hardwarehersteller, ob Ihre physischen Netzwerkadapter Jumbo-Frames unterstützen.

So erstellen Sie einen für Jumbo-Frames aktivierten vSwitch

1 Melden Sie sich direkt an der Konsole Ihres ESX Server 3-Hosts an.

2 Geben Sie den Befehl `esxcfg-vswitch -m <MTU> <vSwitch>` ein, um die MTU-Größe für den vSwitch festzulegen.

Dieser Befehl legt die MTU für alle Uplinks auf diesem vSwitch fest. Die MTU-Größe muss auf die größte MTU-Größe aller virtuellen Netzwerkadapter festgelegt werden, die mit dem vSwitch verbunden sind.

3 Rufen Sie den Befehl `esxcfg-vswitch -l` auf, um eine Liste der vSwitches auf dem Host anzuzeigen, und prüfen Sie, ob die Konfiguration des vSwitches ordnungsgemäß ist.

So erstellen Sie eine für Jumbo-Frames aktivierte VMkernel-Schnittstelle

1 Melden Sie sich direkt an der Konsole Ihres ESX Server 3-Hosts an.

2 Geben Sie den Befehl `esxcfg-vmknic -a -i <IP-Adresse> -n <Netzmaske> -m <MTU> <Portgruppenname>` ein, um eine VMkernel-Verbindung mit Jumbo-Frame-Unterstützung herzustellen.

3 Rufen Sie den Befehl `esxcfg-vmknic -l` auf, um eine Liste der VMkernel-Schnittstellen anzuzeigen, und prüfen Sie, ob die Konfiguration der für Jumbo-Frames aktivierten Schnittstelle ordnungsgemäß ist.

HINWEIS ESX Server 3 unterstützt eine maximale MTU-Größe von 9000.

NetQueue und Netzwerkleistung

NetQueue stellt in ESX Server 3 einen Netzwerkadapter mit mehreren Empfangswarteschlangen bereit. Dadurch kann die Verarbeitung auf mehrere CPUs verteilt werden, wodurch die Empfangsleistung des Netzwerks verbessert wird.

NetQueue steht nur auf den folgenden Systemen mit ausgeführtem Neterion s2io-Treiber zur Verfügung:

- Dell 2950
- HP DL 585G2
- IBM 3850
- IBM 3950

So aktivieren Sie NetQueue auf einem ESX Server 3-Host

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Erweiterte Einstellungen (Advanced Settings)**.

3 Wählen Sie **VMkernel**.

4 Wählen Sie **VMkernel.Boot.netNetQueueEnable**, und klicken Sie auf **OK**.

5 Melden Sie sich direkt an der Konsole Ihres ESX Server 3-Hosts an.

6 Rufen Sie den Befehl `esxcfg-module -e s2io` auf, um das s2io-Modul zu aktivieren.

7 Rufen Sie den Befehl `esxcfg-module -s "intr_type=2 rx_ring_num=8" s2io` auf, um NetQueue für das s2io-Modul zu aktivieren.

8 Starten Sie den ESX Server 3-Host neu.

So deaktivieren Sie NetQueue-Optionen für das s2io-Modul

Melden Sie sich direkt an der Konsole Ihres ESX Server 3-Hosts an, und rufen Sie den Befehl `esxcfg-module -s "" s2io` auf.

Einrichten von MAC-Adressen

Für die von der Servicekonsole, dem VMkernel und den virtuellen Maschinen genutzten virtuellen Netzwerkadapter werden MAC-Adressen generiert. In den meisten Fällen sind diese MAC-Adressen geeignet. In folgenden Fällen ist es jedoch ggf. notwendig, eine MAC-Adresse für einen virtuellen Netzwerkadapter festzulegen:

- Virtuelle Netzwerkadapter auf unterschiedlichen physischen Servern verwenden das gleiche Subnetz, und ihnen wurde die gleiche MAC-Adresse zugewiesen, wodurch ein Konflikt entsteht.
- Sie möchten sicherstellen, dass ein virtueller Netzwerkadapter immer die gleiche MAC-Adresse hat.

Die folgenden Abschnitte beschreiben, wie MAC-Adressen generiert werden und wie Sie die MAC-Adresse für einen virtuellen Netzwerkadapter festlegen können.

Generierung von MAC-Adressen

Jedem virtuellen Netzwerkadapter in einer virtuellen Maschine wird eine eindeutige MAC-Adresse zugewiesen. Eine MAC-Adresse ist eine aus sechs Byte bestehende Zahl. Jedem Hersteller von Netzwerkadaptern wird ein eindeutiges, drei Byte großes Präfix zugewiesen, das OUI (Organizationally Unique Identifier, eindeutiger Bezeichner für Organisationen) genannt wird und das der Hersteller zur Generierung eindeutiger MAC-Adressen verwenden kann.

VMware bietet die folgenden drei OUIs:

- OUI für generierte MAC-Adressen
- OUI für manuell festgelegte MAC-Adressen
- OUI für ältere virtuelle Maschinen (wird jedoch bei ESX Server 3 nicht mehr verwendet)

Die ersten drei Byte der MAC-Adresse, die für jeden virtuellen Netzwerkadapter generiert werden, umfassen die OUI. Der Generierungsalgorithmus für MAC-Adressen erstellt drei weitere Byte. Der Algorithmus garantiert eindeutige MAC-Adressen innerhalb einer Maschine und versucht, eindeutige MAC-Adressen maschinenübergreifend zu erstellen.

Die Netzwerkadapter für jede virtuelle Maschine im gleichen Subnetz müssen eindeutige MAC-Adressen haben. Andernfalls können sie sich unvorhersehbar verhalten. Der Algorithmus beschränkt jederzeit auf allen Servern die Anzahl laufender und angehaltener virtueller Maschinen. Er kann auch nicht alle Fälle identischer MAC-Adressen vermeiden, wenn sich virtuelle Maschinen auf unterschiedlichen physischen Computern ein Subnetz teilen.

Der VMware UUID (Universally Unique Identifier, universaler eindeutiger Bezeichner) generiert MAC-Adressen, die dann auf Konflikte geprüft werden. Die generierten MAC-Adressen bestehen aus drei Teilen: der VMware OUI, der SMBIOS-UUID für den physischen ESX Server 3-Computer und einem Hash, der auf dem Namen der Entität beruht, für welche die MAC-Adresse generiert wird.

Nachdem die MAC-Adresse generiert wurde, ändert sie sich nicht, solange die virtuelle Maschine nicht an einen anderen Speicherort verschoben wird, z. B. in ein anderes Verzeichnis auf dem gleichen Server. Die MAC-Adresse in der Konfigurationsdatei der virtuellen Maschine wird gespeichert. Alle MAC-Adressen, die Netzwerkadaptern laufender oder angehaltener virtueller Maschinen auf einer abgeschalteten physischen Maschine zugewiesen wurden, werden nicht im Abgleich mit MAC-Adressen laufender oder angehaltener virtueller Maschinen geprüft. Es ist möglich, aber unwahrscheinlich, dass beim Hochfahren einer virtuellen Maschine eine andere MAC-Adresse angefordert wird. Diese Anforderung wird durch einen Konflikt mit einer virtuellen Maschine verursacht, die hochgefahren wurde, während diese virtuelle Maschine ausgeschaltet war.

Festlegen von MAC-Adressen

Um die Begrenzung auf 256 virtuelle Netzwerkadapter pro physischem Computer zu umgehen und mögliche MAC-Adressenkonflikte zwischen virtuellen Maschinen zu vermeiden, können Systemadministratoren MAC-Adressen manuell zuweisen. VMware verwendet folgenden OUI für manuell generierte MAC-Adressen: 00:50:56.

Der Adressbereich für die MAC-Adresse lautet

```
00:50:56:00:00:00–00:50:56:3F:FF:FF
```

Sie können die Adressen festlegen, indem Sie der Konfigurationsdatei der virtuellen Maschine folgende Zeile hinzufügen:

```
ethernet<Nummer>.address = 00:50:56:XX:YY:ZZ
```

wobei <Nummer> die Zahl des Ethernet-Adapters angibt, XX eine gültige Hexadezimalzahl von 00 bis 3F ist und YY und ZZ gültige Hexadezimalzahlen von 00 bis FF sind. Der Wert für XX darf nicht größer als 3F sein, um Konflikte mit MAC-Adressen zu vermeiden, die von VMware Workstation und VMware GSX Server generiert werden. Der Höchstwert für eine manuell generierte MAC-Adresse lautet

```
ethernet<Nummer>.address = 00:50:56:3F:FF:FF
```

Sie müssen außerdem folgende Option in der Konfigurationsdatei der virtuellen Maschine festlegen:

```
ethernet<Nummer>.addressType="static"
```

Da virtuelle Maschinen von VMware ESX Server 3 keine beliebigen MAC-Adressen unterstützen, muss das oben genannte Format eingehalten werden. Wenn Sie für Ihre nicht veränderlichen Adressen einen eindeutigen Wert für XX:YY:ZZ festlegen, dürften keine Konflikte zwischen den automatisch zugewiesenen und den manuell zugewiesenen MAC-Adressen auftreten.

Verwenden von MAC-Adressen

Sie können den Netzwerkkarten einer deaktivierten virtuellen Maschine über den VI-Client statische MAC-Adressen zuweisen.

So richten Sie eine MAC-Adresse ein

1. Melden Sie sich am VI-Client an, und wählen Sie die virtuelle Maschine in der Bestandsliste aus.
2. Klicken Sie auf der Registerkarte **Übersicht (Summary)** auf **Einstellungen bearbeiten (Edit Settings)**.
3. Wählen Sie in der Liste **Hardware** den Netzwerkadapter aus.
4. Wählen Sie unter **MAC-Adresse (MAC Address)** die Option **Manuell (Manual)** aus.
5. Geben Sie die gewünschte statische MAC-Adresse ein, und klicken Sie auf **OK**.

Optimale Vorgehensweisen und Tipps für Netzwerke

In diesem Abschnitt finden Sie Informationen zu folgenden Themen:

- Optimale Vorgehensweisen für Netzwerke
- Netzwerktipps

Optimale Vorgehensweisen für Netzwerke

Ziehen Sie folgende optimale Vorgehensweisen für die Konfiguration Ihres Netzwerks in Betracht:

- Trennen Sie die Netzwerkdienste voneinander, um mehr Sicherheit und eine höhere Leistung zu erreichen.

  Wenn eine bestimmte Gruppe virtueller Maschinen höchste Leistung bieten soll, schließen Sie sie an eine eigene physische Netzwerkkarte an. Durch diese Abtrennung kann ein Teil der Gesamtarbeitslast des Netzwerks gleichmäßiger auf mehrere CPUs verteilt werden. Die isolierten virtuellen Maschinen sind dann beispielsweise besser in der Lage, den Datenverkehr eines Webclients zu verarbeiten.

- Die unten aufgeführten Empfehlungen können entweder durch die Verwendung von VLANs zur Aufteilung eines physischen Netzwerks in Segmente oder durch die Verwendung getrennter physischer Netzwerke umgesetzt werden (die zweite Variante ist dabei zu bevorzugen).

  - Ein wichtiger Bestandteil der Absicherung des ESX Server 3-Systems besteht darin, dass die Servicekonsole über ein eigenes Netzwerk verfügt. Die Netzwerkanbindung der Servicekonsole sollte genauso gehandhabt werden wie Geräte für den Fernzugriff auf Server, da die Übernahme der Servicekonsole einem Angreifer die vollständige Kontrolle über alle virtuellen Maschinen auf dem System ermöglicht.

  - Es ist wichtig, dass die VMotion-Verbindung über ein eigenes, für diesen Zweck vorgesehenes Netzwerk verfügt, da die Speicherinhalte des Gastbetriebssystems bei der Migration mit VMotion über das Netzwerk übertragen werden.

Mounten von NFS-Volumes

Die Weise, wie der ESX Server 3 auf NFS-Speicher von ISO-Images zugreift, die als virtuelle CD-ROMs für virtuelle Maschinen verwendet werden, unterscheidet sich von der Weise, wie das in ESX Server 2.x geschah.

ESX Server 3 unterstützt das VMkernel-basierte NFS-Mounting. Bei dem neuen Modell wird das NFS-Volume mit den ISO-Images über die NFS-Funktion des VMkernels gemounted. Alle so gemounteten NFS-Volumes werden im VI-Client als Datenspeicher angezeigt. Mit dem Konfigurations-Editor der virtuellen Maschine können Sie das Dateisystem der Servicekonsole nach ISO-Images durchsuchen, die als virtuelle CD-ROM-Laufwerke verwendet werden sollen.

Netzwerktipps

Beachten Sie auch die folgenden Netzwerktipps:

- Um Netzwerkdienste physisch zu trennen und eine bestimmte Gruppe von Netzwerkkarten einem bestimmten Netzwerkdienst zuzuweisen, erstellen Sie einen vSwitch für jeden Dienst. Wenn das nicht möglich ist, können die Dienste auf einem vSwitch voneinander getrennt werden, indem sie Portgruppen mit unterschiedlichen VLAN-IDs zugeordnet werden. In jedem Fall sollte der Netzwerkadministrator bestätigen, dass die gewählten Netzwerke oder VLANs vom Rest der Umgebung isoliert sind, d. h. dass keine Router daran angeschlossen sind.
- Sie können Netzwerkkarten zum vSwitch hinzufügen oder davon entfernen, ohne dass die virtuellen Maschinen oder die Netzwerkdienste hinter diesem vSwitch beeinflusst werden. Wenn Sie die gesamte ausgeführte Hardware entfernen, können die virtuellen Maschinen weiter untereinander kommunizieren. Wenn Sie eine Netzwerkkarte intakt lassen, können alle virtuellen Maschinen weiterhin auf das physische Netzwerk zugreifen.
- Um virtuelle Maschinen in Gruppen einzuteilen, verwenden Sie in der Gruppierungsrichtlinie Portgruppen mit unterschiedlichen Sätzen aktiver Adapter. Diese Gruppen können unterschiedliche Adapter verwenden, wenn alle Adapter funktionsfähig sind. Im Fall eines Netzwerk- oder Hardwareausfalls teilen sie sich die Adapter jedoch wieder.
- Um die empfindlichsten virtuellen Maschinen zu schützen, installieren Sie Firewalls auf virtuellen Maschinen, die den Datenverkehr zwischen virtuellen Netzwerken mit Uplinks zu physischen Netzwerken und reinen virtuellen Netzwerken ohne Uplinks weiterleiten.

Netzwerkszenarien und Problemlösung

4

Dieses Kapitel beschreibt die allgemeine Netzwerkkonfiguration und Problemlösungsszenarien.

In diesem Kapitel werden folgende Themen behandelt:

- „Netzwerkkonfiguration für Software-iSCSI-Speicher“ auf Seite 76
- „Konfigurieren des Netzwerks auf Blade-Servern“ auf Seite 81
- „Fehlerbehebung“ auf Seite 85

Netzwerkkonfiguration für Software-iSCSI-Speicher

Der Speicher, den Sie für einen ESX Server 3-Host konfigurieren, kann ein oder mehrere SANs (Speichernetzwerke) umfassen, die iSCSI-Speicher verwenden. iSCSI ist ein Instrument für den Zugriff auf SCSI-Geräte und zum Austausch von Datensätzen, indem das TCP/IP-Protokoll über einen Netzwerkport und nicht über einen direkten Anschluss an ein SCSI-Gerät eingesetzt wird. Bei iSCSI-Übertragungen werden Raw-SCSI-Datenblöcke in iSCSI-Datensätze gekapselt und an das Gerät oder den Benutzer übertragen, das/der die Anforderung gestellt hat.

HINWEIS In ESX Server 3.5 steht Software-initiiertes iSCSI über 10GigE-Netzwerkadapter nicht zur Verfügung.

Bevor Sie den iSCSI-Speicher konfigurieren können, müssen Sie einen VMkernel-Port für das iSCSI-Netzwerk und die Verbindung der Servicekonsole zum iSCSI-Netzwerk anlegen.

So legen Sie einen VMkernel-Port für Software-iSCSI an

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

  Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.

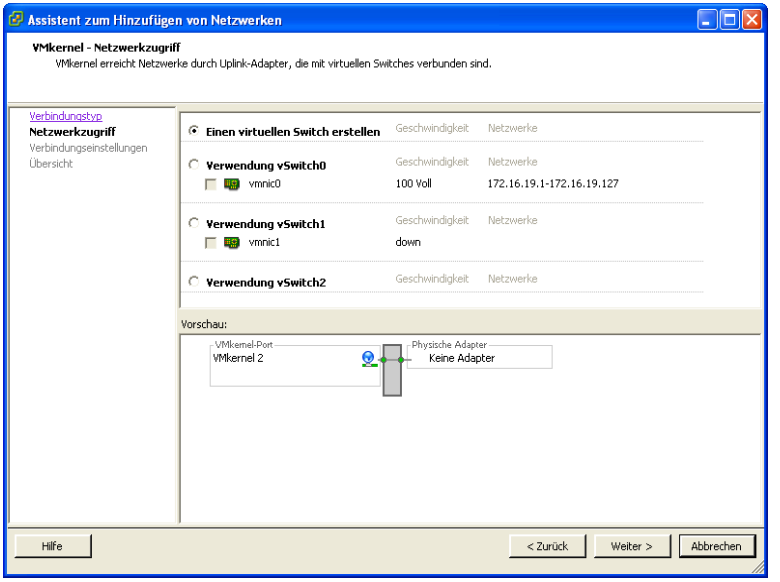
3 Klicken Sie auf **Netzwerk hinzufügen (Add Networking)**.

4 Wählen Sie **VMkernel** aus, und klicken Sie auf **Weiter (Next)**.

  Das Dialogfeld **Netzwerkzugriff (Network Access)** wird angezeigt. Auf dieser Seite können Sie den VMkernel, der die Dienste für den iSCSI-Speicher ausführt, an das physische Netzwerk anschließen.

5 Wählen Sie den vSwitch aus, den Sie verwenden möchten, oder klicken Sie auf **Einen virtuellen Switch erstellen (Create a virtual switch)**.

6 Aktivieren Sie die Kontrollkästchen für die Netzwerkadapter, die Ihr vSwitch verwenden soll.



Die Auswahlmöglichkeiten werden im Bereich **Vorschau (Preview)** angezeigt.

Wählen Sie für jeden vSwitch Adapter aus, sodass die virtuellen Maschinen, die an diese Adapter angeschlossen sind, auf das ordnungsgemäße Ethernet-Segment zugreifen können. Wenn unter **Einen virtuellen Switch erstellen (Create a virtual switch)** keine Adapter angezeigt werden, bedeutet dies, dass alle Netzwerkadapter im System von vorhandenen vSwitches verwendet werden.

Weitere Informationen zum Verschieben von Netzwerkadaptern zwischen vSwitches finden Sie unter „So fügen Sie Uplink-Adapter hinzu“ auf Seite 45.

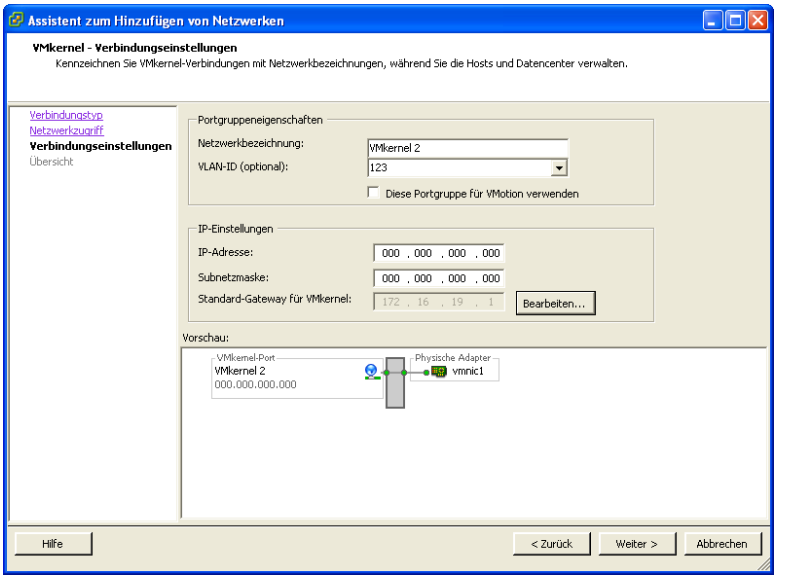
HINWEIS Verwenden Sie iSCSI nicht bei 100-MB-Netzwerkadaptern.

7 Klicken Sie auf **Weiter (Next)**.

8 Wählen Sie unter **Eigenschaften der Portgruppe (Port Group Properties)** eine Netzwerkbezeichnung und eine VLAN-ID aus bzw. geben Sie diese ein.

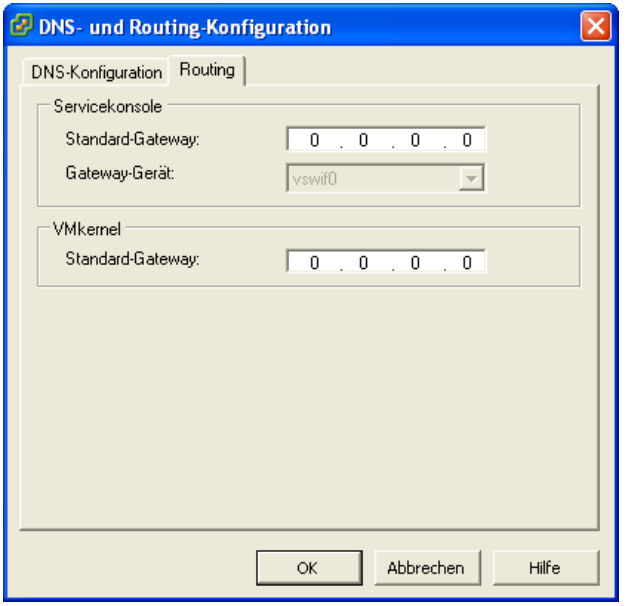
Netzwerkbezeichnung (Network Label). Ein Name, der die Portgruppe bezeichnet, die erstellt wird. Es handelt sich dabei um die Bezeichnung, die Sie bei der Konfiguration eines virtuellen Adapters, der an diese Portgruppe angeschlossen wird, beim Konfigurieren eines iSCSI-Speichers festlegen.

VLAN-ID (VLAN ID). Bezeichnet das VLAN, das für den Netzwerkdatenverkehr der Portgruppe verwendet wird. VLAN-IDs sind nicht erforderlich. Falls Sie nicht wissen, ob sie benötigt werden, wenden Sie sich an den Netzwerkadministrator.



9 Klicken Sie unter **IP-Einstellungen (IP Settings)** auf **Bearbeiten (Edit)**, um **VMkernel-Standardgateway (VMkernel Default Gateway)** für iSCSI anzugeben.

Auf der Registerkarte **Routing** benötigen die Servicekonsole und der VMkernel jeweils eigene Angaben zum Gateway.



HINWEIS Legen Sie ein Standardgateway für den Port fest, den Sie erstellt haben. Sie müssen eine gültige statische IP-Adresse angeben, um den VMkernel-Stapel zu konfigurieren.

10 Klicken Sie auf **OK**.

11 Klicken Sie auf **Weiter (Next)**.

12 Klicken Sie auf **Zurück (Back)**, um Änderungen vorzunehmen.

13 Überprüfen Sie die Änderungen im Dialogfeld **Bereit zum Abschließen (Ready to Complete)**, und klicken Sie auf **Fertig (Finish)**.

Nach Anlegen des VMkernel-Ports für iSCSI müssen Sie eine Verbindung der Servicekonsole auf demselben vSwitch anlegen, auf dem sich VMkernel-Port befindet.

So konfigurieren Sie eine Verbindung der Servicekonsole zum Software-iSCSI-Speicher

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

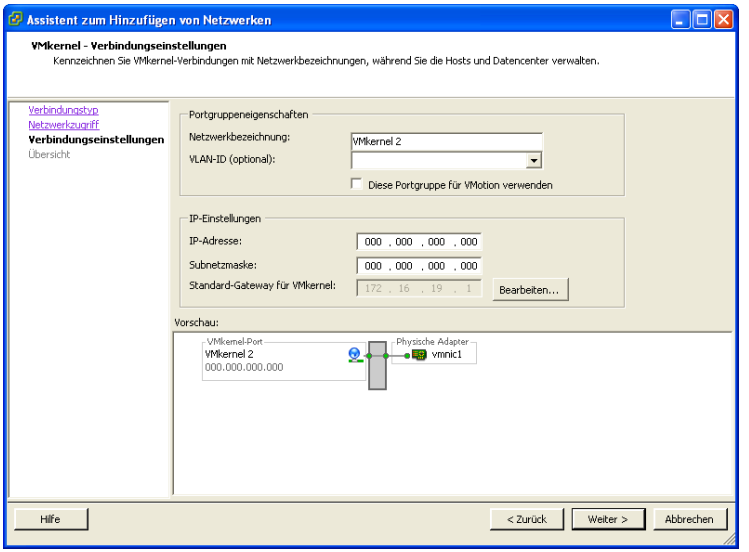
2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.

3 Klicken Sie auf der rechten Seite des Bildschirms auf **Eigenschaften (Properties)** für den vSwitch, der dem VMkernel-Port zugeordnet ist, den Sie gerade angelegt haben.

4 Klicken Sie auf der Registerkarte **Port** auf **Hinzufügen (Add)**.

5 Wählen Sie als Verbindungstyp **Servicekonsole (Service Console)**, und klicken Sie auf **Weiter (Next)**.

6 Geben Sie unter **Eigenschaften der Portgruppe (Port Group Properties)** eine Netzwerkbezeichnung für die zu erstellende Portgruppe ein.



Neuere Ports und Portgruppen werden im vSwitch-Diagramm oben angezeigt.

7 Geben Sie die **IP-Adresse (IP Address)** und die **Subnetzmaske (Subnet Mask)** ein, oder aktivieren Sie die DHCP-Option **IP-Einstellung automatisch beziehen (Obtain IP setting automatically)** für die IP-Adresse und die Subnetzmaske. Diese IP-Adresse muss sich von der für den VMkernel gewählten unterscheiden.

8 Klicken Sie auf **Bearbeiten (Edit)**, um **Standard-Gateway der Servicekonsole (Service Console Default Gateway)** festzulegen.

Siehe „So legen Sie das Standard-Gateway fest“ auf Seite 37.

9 Klicken Sie auf **Weiter (Next)**.

10 Überprüfen Sie die ordnungsgemäße Konfiguration des vSwitches noch einmal, und klicken Sie dann auf **Fertig (Finish)**.

Nachdem Sie einen VMkernel-Port und die Servicekonsolenverbindung erstellt haben, können Sie den Software-iSCSI-Speicher aktivieren und konfigurieren. Weitere Informationen zur Konfiguration von iSCSI-Adaptern und -Speichern finden Sie unter „iSCSI-Speicher“ auf Seite 116.

Konfigurieren des Netzwerks auf Blade-Servern

Da Blade-Server mitunter nur über eine begrenzte Anzahl an Netzwerkadaptern verfügen, ist es ggf. erforderlich, VLANs für einen separaten Datenverkehr für die Servicekonsole, VMotion, den IP-Speicher und verschiedene Gruppen virtueller Maschinen zu verwenden. VMware empfiehlt ausdrücklich, aus Sicherheitsgründen eigene Netzwerke für die Servicekonsole und VMotion anzulegen. Wenn Sie getrennten vSwitches zu diesem Zweck physische Adapter zuweisen, müssen Sie möglicherweise auf redundante (gruppierte) Verbindungen oder die Isolierung der verschiedenen Netzwerkclients oder auf beides verzichten. Mit VLANs können Sie eine Netzwerksegmentierung erreichen, ohne mehrere physische Adapter verwenden zu müssen.

Damit der Netzwerk-Blade eines Blade-Servers die ESX Server 3-Portgruppe mit VLAN-getaggtem Datenverkehr unterstützt, müssen sie das Blade so konfigurieren, dass es 802.1Q unterstützt und den Port als getaggten Port konfigurieren.

Die Methode zum Konfigurieren eines Ports als getaggten Port ist von Server zu Server verschieden. Die folgende Liste beschreibt die Konfiguration eines ggetaggten Ports auf drei der am häufigsten verwendeten Blade-Server:

HP Blade	Setzen Sie **VLAN-Tagging (VLAN Tagging)** für den Port auf **Aktiviert (enabled)**.
Dell PowerEdge	Setzen Sie den Port auf **Getaggt (Tagged)**.
IBM eServer Blade Center	Wählen Sie in der Portkonfiguration **Kennzeichnung (Tag)** aus.

So konfigurieren Sie eine Portgruppe für virtuelle Maschinen mit VLAN auf einem Blade-Server

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.

3 Klicken Sie auf auf der rechten Seite des Bildschirms auf **Eigenschaften (Properties)** für den vSwitch, der der Servicekonsole zugeordnet ist.

4 Klicken Sie auf der Registerkarte **Port** auf **Hinzufügen (Add)**.

5 Wählen Sie als Verbindungstyp **Virtuelle Maschinen (Virtual Machines)** (Standard).

6 Klicken Sie auf **Weiter (Next)**.

7 Geben Sie unter **Eigenschaften der Portgruppe (Port Group Properties)** eine Netzwerkbezeichnung für die zu erstellende Portgruppe ein.

Mit den Netzwerkbezeichnungen können Sie migrationsfähige Verbindungen für zwei oder mehr Hosts kennzeichnen.

8 Geben Sie im Feld **VLAN-ID (VLAN ID)** eine Zahl von 1 bis 4094 ein.

Wenn Sie sich nicht sicher sind, was hier eingegeben werden muss, lassen Sie das Feld frei, oder wenden Sie sich an Ihren Netzwerkadministrator.

9 Klicken Sie auf **Weiter (Next)**.

10 Überprüfen Sie die ordnungsgemäße Konfiguration des vSwitches noch einmal, und klicken Sie dann auf **Fertig (Finish)**.

So konfigurieren Sie einen VMkernel-Port mit VLAN auf einem Blade-Server

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

Die Seite **Hardwarekonfiguration (hardware configuration)** für diesen Server wird angezeigt.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Netzwerk (Networking)**.

3 Klicken Sie auf auf der rechten Seite des Bildschirms auf **Eigenschaften (Properties)** für den vSwitch, der der Servicekonsole zugeordnet ist.

4 Klicken Sie auf der Registerkarte **Ports** auf **Hinzufügen (Add)**.

5 Wählen Sie **VMkernel** aus, und klicken Sie auf **Weiter (Next)**.

Über diese Option können Sie den VMkernel, der Dienste für VMotion und IP-Speicher (NFS oder iSCSI) ausführt, an ein physisches Netzwerk anschließen.

6 Wählen Sie unter **Eigenschaften der Portgruppe (Port Group Properties)** eine Netzwerkbezeichnung und eine VLAN-ID aus bzw. geben Sie diese ein.

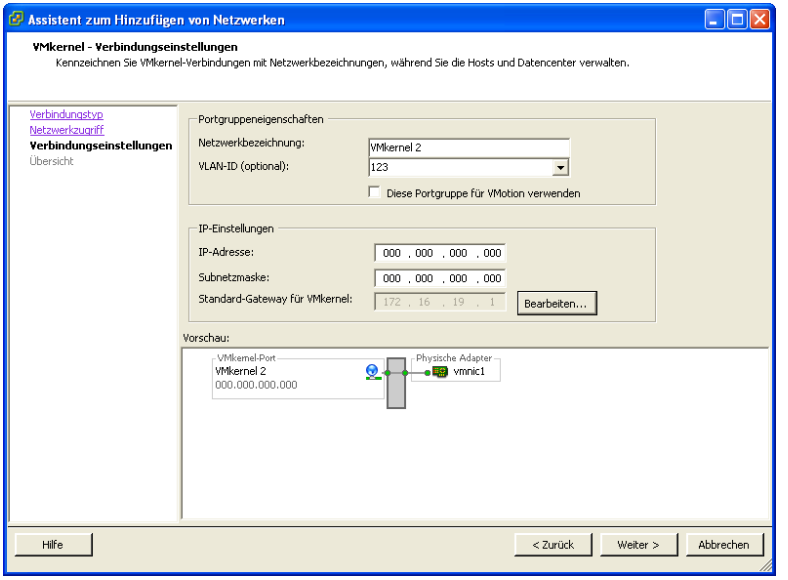
Netzwerkbezeichnung (Network Label). Ein Name, der die Portgruppe bezeichnet, die erstellt wird. Es handelt sich dabei um die Bezeichnung, die Sie bei der Konfiguration von VMkernel-Diensten wie VMotion und IP-Speicher während der Konfiguration des virtuellen Adapters festlegen, der an diese Portgruppe angeschlossen wird.

VLAN-ID (VLAN ID). Bezeichnet das VLAN, das für den Netzwerkdatenverkehr der Portgruppe verwendet wird.

7 Aktivieren Sie **Diese Portgruppe für VMotion verwenden (Use this port group for VMotion)**, damit diese Portgruppe einem anderen ESX Server 3-Host melden kann, dass sie als Netzwerkverbindung dient, an die VMotion-Datenverkehr gesendet werden soll.

Auf jedem ESX Server 3-Host kann diese Eigenschaft nur für eine VMotion- und IP-Speicher-Portgruppe aktiviert werden. Wenn diese Eigenschaft für keine der

Portgruppen aktiviert wurde, ist eine VMotion-Migration auf diesen Host nicht möglich.



8 Klicken Sie unter **IP-Einstellungen (IP Settings)** auf **Bearbeiten (Edit)**, um **Standard-Gateway für VMkernel (VMkernel Default Gateway)** für VMkernel-Dienste wie VMotion, NAS und iSCSI einzurichten.

HINWEIS Legen Sie ein Standardgateway für den Port fest, den Sie erstellt haben. VirtualCenter 2 verhält sich anders als VirtualCenter 1.x. Sie müssen eine gültige IP-Adresse und keine Pseudoadresse angeben, um den VMkernel-IP-Stapel zu konfigurieren.

Auf der Registerkarte **DNS-Konfiguration (DNS Configuration)** ist im Namensfeld standardmäßig der Hostname eingetragen. Auch die DNS-Server-Adressen und die Domäne, die während der Installation angegeben wurden, werden automatisch eingetragen.

Auf der Registerkarte **Routing** benötigen die Servicekonsole und der VMkernel jeweils eigene Angaben zum Gateway. Ein Gateway ist zur Anbindung an Computer notwendig, die sich nicht im gleichen IP-Subnetz wie die Servicekonsole oder der VMkernel befinden.

Statische IP-Einstellungen sind standardmäßig festgelegt.

9 Klicken Sie auf **OK**.

10 Klicken Sie auf **Weiter (Next)**.

11 Klicken Sie auf **Zurück (Back)**, um Änderungen vorzunehmen.

12 Überprüfen Sie die Änderungen im Dialogfeld **Bereit zum Abschließen (Ready to Complete)**, und klicken Sie auf **Fertig (Finish)**.

Fehlerbehebung

Der folgende Abschnitt führt Sie durch die Fehlerbehebung bei typischen Netzwerkproblemen.

Fehlerbehebung bei der Vernetzung der Servicekonsole

Wenn bestimmte Teile der Netzwerkkonfiguration der Servicekonsole falsch konfiguriert sind, können Sie über den VI-Client nicht mehr auf den ESX Server 3-Host zugreifen. In diesem Fall können Sie die Netzwerkeinstellungen neu konfigurieren, indem Sie direkt auf die Servicekonsole zugreifen und folgenden Befehle aufrufen:

- `esxcfg-vswif -l`

  Gibt eine Liste der bestehenden Netzwerkschnittstellen der Servicekonsole aus.

  Prüfen Sie, ob `vswif0` vorhanden ist und die aktuelle IP-Adresse und Netzmaske stimmen.

- `esxcfg-vswitch -l`

  Gibt eine Liste der bestehenden Konfigurationen für die virtuellen Switches aus.

  Prüfen Sie, ob der Uplink-Adapter, der für die Servicekonsole konfiguriert wurde, mit dem gewünschten physischen Netzwerk verbunden ist.

- `exscfg-nics -l`

  Gibt eine Liste der aktuellen Netzwerkadapter aus.

  Prüfen Sie, ob der Uplink-Adapter, der für die Servicekonsole konfiguriert wurde, aktiv ist und Geschwindigkeit und Duplex stimmen.

- `esxcfg-nics -s <Geschwindigkeit> <Netzwerkkarte>`

  Ändert die Geschwindigkeit eines Netzwerkadapters.

- `esxcfg-nics -d <Duplex> <Netzwerkkarte>`

  Ändert den Duplex eines Netzwerkadapters.

- `esxcfg-vswif -i <neue IP-Adresse> vswifX`

  Ändert die IP-Adresse der Servicekonsole.

- `esxcfg-vswif -n <neue Subnetzmaske> vswifX`

  Ändert die Subnetzmaske der Servicekonsole.

- `esxcfg-vswitch -U <old vmnic> <service console vswitch>`

  Entfernt den Uplink für die Servicekonsole.

- `esxcfg-vswitch -L <new vmnic> <service console vswitch>`

  Ändert den Uplink für die Servicekonsole.

Wenn Sie bei `esxcfg-*` Befehlen lange warten müssen, kann dies an einer falschen DNS-Einstellung liegen. Die `esxcfg-*` Befehle setzen voraus, dass DNS so konfiguriert ist, dass die Namensauflösung des lokalen Servers ordnungsgemäß funktioniert. Dies setzt wiederum voraus, dass die Datei `/etc/hosts` einen Eintrag für die konfigurierte IP-Adresse und die „localhost"-Adresse 127.0.0.1 enthält.

Fehlerbehebung bei der Netzwerkadapterkonfiguration

Das Hinzufügen eines neuen Netzwerkadapters kann in bestimmten Fällen zum Verlust der Netzwerkverbindung der Servicekonsole sowie der Verwaltbarkeit mit dem VI-Client führen, da Netzwerkadapter umbenannt wurden.

Wenn dies der Fall ist, müssen Sie die betroffenen Netzwerkadapter, die die Servicekonsole nutzen, umbenennen.

So benennen Sie Netzwerkadapter über die Servicekonsole um

1. Melden Sie sich direkt an der Konsole Ihres ESX Server 3-Hosts an.
2. Verwenden Sie den Befehl `esxcfg-nics -l`, um anzuzeigen, welche Namen Ihren Netzwerkadaptern zugewiesen wurden.
3. Verwenden Sie den Befehl `esxcfg-vswitch -l`, um anzuzeigen, welche vSwitches, sofern vorhanden, jetzt den Gerätenamen zugewiesen sind, die nicht mehr durch `esxcfg-nics` angezeigt werden.
4. Verwenden Sie den Befehl `esxcfg-vswitch -U <old vmnic name> <vswitch>`, um Netzwerkadapter zu entfernen, die umbenannt worden sind.
5. Verwenden Sie den Befehl `esxcfg-vswitch -L <new vmnic name> <vswitch>`, um die Netzwerkadapter mit ordnungsgemäßen Namen wieder hinzuzufügen.

Fehlerbehebung bei der Konfiguration physischer Switches

In manchen Fällen kann bei einem Failover oder Failback die Verbindung zum vSwitch getrennt werden. Dadurch werden die MAC-Adressen, die von diesem vSwitch

zugeordneten virtuellen Maschinen verwendet werden, auf einem anderen Switchport angezeigt als zuvor.

Um dieses Problem zu vermeiden, setzen Sie Ihren physischen Switch auf den Portfast- oder Portfast-Trunk-Modus.

Fehlerbehebung bei der Portgruppenkonfiguration

Das Umbenennen einer Portgruppe bei bereits mit dieser Portgruppe verbundenen virtuellen Maschinen kann zu einer ungültigen Netzwerkkonfiguration virtueller Maschinen führen, die für eine Verbindung mit dieser Portgruppe konfiguriert sind.

Die Verbindung virtueller Netzwerkadapter mit den Portgruppen erfolgt anhand des Namens, und der Name wird in der Konfiguration der virtuellen Maschine gespeichert. Das Ändern des Namens einer Portgruppe führt nicht zu einer Massenneukonfiguration aller virtuellen Maschinen, die mit dieser Portgruppe verbunden sind. Virtuelle Maschinen, die bereits eingeschaltet sind, werden weiterhin funktionieren, bis sie ausgeschaltet werden, da ihre Verbindungen zum Netzwerk bereits hergestellt sind.

Vermeiden Sie das Umbenennen bereits verwendeter Netzwerke. Nach dem Umbenennen einer Portgruppe müssen Sie jede zugeordnete virtuelle Maschine über die Servicekonsole neu konfigurieren, um den neuen Portgruppennamen entsprechend zu berücksichtigen.

Speicher

Einführung in die Speicherung

5

Der Abschnitt zur Speicherung enthält eine Übersicht der verfügbaren Speicheroptionen für ESX Server 3 und erläutert die Konfiguration Ihres ESX Server 3-Systems für die Nutzung und Verwaltung verschiedener Speichertypen.

Informationen zu bestimmten Aktivitäten, die ein Speicheradministrator ggf. für Speicherarrays ausführen muss, finden Sie im *SAN-Konfigurationshandbuch (für Fiber Channel)* und *SAN-Konfigurationshandbuch (für iSCSI)*.

In diesem Kapitel werden folgende Themen behandelt:

- „Speicher – Übersicht“ auf Seite 92
- „Physische Speichertypen“ auf Seite 93
- „Unterstützte Speicheradapter“ auf Seite 95
- „Datenspeicher“ auf Seite 95
- „Vergleich der Speichertypen“ auf Seite 102
- „Anzeigen der Speicherinformationen im VMware Infrastructure-Client“ auf Seite 102
- „Konfigurieren und Verwalten von Speichern“ auf Seite 106

Speicher – Übersicht

Eine virtuelle Maschine in ESX Server 3 verwendet eine virtuelle Festplatte, um das Betriebssystem, die Programmdateien und andere Daten für ihren Betrieb zu speichern. Eine virtuelle Festplatte ist eine große physische Datei bzw. Zusammenstellung von Dateien, die sich so einfach wie jede andere Datei kopieren, verschieben, archivieren und sichern lässt. Zum Speichern virtueller Festplattendateien und Bearbeiten der Dateien benötigt ESX Server 3 dediziert zugewiesenen Speicherplatz.

ESX Server 3 nutzt Speicherplatz auf einer Vielzahl physischer Speichergeräte, so z. B. die internen und externen Speichergeräte Ihres Hosts oder an das Netzwerk angeschlossene Speichergeräte. Das Speichergerät ist eine physische Festplatte oder ein Festplattenarray, das für spezifische Aufgaben zum Speichern und Schützen von Daten reserviert ist.

ESX Server 3 kann Speichergeräte, auf die Zugriff besteht, erkennen und als Datenspeicher formatieren. Der Datenspeicher ist ein spezieller logischer Container (ähnlich einem Dateisystem auf einem logischen Volume), in dem ESX Server 3 virtuelle Festplattendateien und andere Dateien ablegt, in denen wesentliche Komponenten einer virtuellen Maschine gekapselt werden. Die Datenspeicher werden auf verschiedenen Geräten bereitgestellt, wobei Angaben zu den einzelnen Speicherungsprodukten verborgen bleiben, und bieten ein einheitliches Modell für die Speicherungen der Dateien virtueller Maschinen.

Mit dem VI-Client können Sie Datenspeicher im Vorfeld auf allen Speichergeräten einrichten, die Ihr ESX Server 3 erkennt.

Die folgenden Kapitel enthalten Informationen zum Zugriff auf die und zur Konfiguration der Speichergeräte sowie zum Erstellen und Verwalten von Datenspeichern.

- „Speicherkonfiguration“ auf Seite 109
- „Speicherverwaltung“ auf Seite 141

Nachdem Sie die Datenspeicher erstellt haben, können Sie die Dateien virtueller Maschinen darin speichern. Weitere Informationen zum Erstellen virtuellen Maschinen finden Sie unter *Grundlagen der Systemverwaltung*.

Physische Speichertypen

Die Verwaltung des ESX Server 3-Datenspeichers beginnt mit dem Speicherplatz, den der Speicheradministrator auf verschiedenen Speichergeräten zuweist.

ESX Server 3 unterstützt folgende Typen von Speichergeräten:

- **Lokal** – Dateien virtueller Maschinen werden auf internen oder externen Speichergeräten oder Arrays gespeichert, die über eine Direktverbindung an den ESX Server 3-Host angeschlossen sind.
- **Vernetzt** – Dateien virtueller Maschinen werden auf internen oder externen Speichergeräten oder Arrays gespeichert, die sich außerhalb des ESX Server 3-Hosts befinden. Der Host kommuniziert mit den vernetzten Geräten über ein Hochgeschwindigkeitsnetzwerk.

Lokaler Speicher

Lokale Speichergeräte können interne Festplatte innerhalb des ESX Server 3-Hosts oder externe Speichersysteme außerhalb des Hosts sein, die direkt mit dem Host verbunden sind.

Lokale Speichergeräte benötigen kein Speichernetzwerk für die Kommunikation mit dem ESX Server 3. Benötigt werden lediglich ein an das Speichergerät angeschlossenes Kabel und, falls erforderlich, ein kompatibler HBA im ESX Server 3-Host.

In der Regel können mehrere ESX Server 3-Hosts an ein einzelnes lokales Speichersystem angeschlossen werden. Die tatsächliche Anzahl der Hosts, die Sie anschließen, hängt vom Typ des Speichergeräts und der verwendeten Topologie ab.

Viele lokale Speichersysteme unterstützen redundante Verbindungspfade, um Fehlertoleranz zu gewährleisten. Siehe „Verwalten mehrerer Pfade“ auf Seite 146.

Wenn mehrere ESX Server 3-Hosts an die lokale Speichereinheit angeschlossen sind, können Sie im nicht gemeinsamen Nutzungsmodus auf Speicher-LUNs zugreifen. Der nicht gemeinsame Nutzungsmodus lässt nicht zu, dass mehrere ESX Server 3-Hosts gleichzeitig auf denselben VMFS-Datenspeicher zugreifen. Es gibt jedoch verschiedene SAS-Speichersysteme, die einen gemeinsamen Zugriff auf mehrere ESX Server 3i-Hosts bieten. Diese Art des Zugriffs ermöglicht mehreren ESX Server 3i-Hosts, auf denselben VMFS-Dateispeicher auf einer LUN zuzugreifen. Siehe „Gemeinsames Nutzen eines VMFS-Volumes durch mehrere ESX Server 3-Systeme“ auf Seite 99.

ESX Server 3 unterstützt verschiedene interne und externe lokale Speichergeräte, einschließlich SCSI-, IDE-, SATA- und SAS-Speichersystemen. Unabhängig vom gewählten Speichertyp verbirgt ESX Server 3 eine physische Speicherebene vor den virtuellen Maschinen.

Beachten Sie beim Einrichten des lokalen Speichers Folgendes:

- Virtuelle Maschinen können nicht auf IDE-/ATA-Laufwerken gespeichert werden.
- Verwenden Sie lokalen internen und externen SATA-Speicher nur im nicht gemeinsamen Nutzungsmodus. SATA-Speicher unterstützt nicht die gemeinsame Nutzung derselben LUNs und deshalb nicht denselben VMFS-Dateispeicher für mehrere ESX Server 3-Hosts.

  Stellen Sie bei der Verwendung von SATA-Speicher sicher, dass die SATA-Laufwerke über unterstützte SATA-/SAS-Dual-Controller angeschlossen sind.
- Verschiedene SAS-Speichersysteme unterstützen den gemeinsamen Zugriff auf dieselben LUNs (und deshalb auf dieselben VMFS-Dateispeicher) für mehrere ESX Server 3-Hosts.

Informationen zu unterstützten lokalen Speichergeräten finden Sie im *Handbuch zur E/A-Kompatibilität* unter www.vmware.com/support/pubs/vi_pubs.html.

Netzwerkspeicher

Netzwerkspeichergeräte sind externe Speichergeräte oder Arrays, auf denen der ESX Server 3-Host Dateien virtueller Maschinen extern speichert. Der ESX Server 3-Host greift auf diese Geräte über ein Hochgeschwindigkeitsnetzwerk zu.

ESX Server 3 unterstützt folgende Netzwerkspeichertechnologien:

- **Fibre-Channel (FC)** – Speichert Dateien virtueller Maschinen extern in einem FC-Speichernetzwerk (Storage Area Network, SAN). Ein FC-SAN ist ein spezielles Hochgeschwindigkeitsnetzwerk, das Ihre ESX Server 3-Hosts mit Hochleistungsspeichergeräten verbindet. Das Netzwerk nutzt das Fibre-Channel-Protokoll zur Übertragung von SCSI-Datenverkehr virtueller Maschinen au FC-SAN-Geräte.

  Für den Anschluss an das FC-SAN muss der ESX Server 3-Host mit Fibre-Channel-HBAs (Hostbusadaptern) und (außer Sie arbeiten mit Fibre-Channel-Direktverbindungsspeicher) mit Fibre-Channel-Switches ausgestattet sein, die die Weiterleitung der zu speichernden Daten unterstützen.
- **Internet SCSI (iSCSI)** – Speichert Dateien virtueller Maschinen auf externen iSCSI-Speichergeräten. iSCSI packt SCSI-Speicherdatenverkehr in das TCP/IP-Protokoll, sodass dieser über standardmäßige TCP/IP-Netzwerke anstatt über ein spezielles Fibre-Channel-Netzwerk übertragen werden kann. Bei einer iSCSI-Verbindung dient der ESX Server 3-Host als *Initiator*, der mit einem *Ziel* kommuniziert, das sich in externen iSCSI-Speichersystemen befindet.

ESX Server 3 unterstützt folgende Arten von iSCSI-Verbindungen:

- **Hardware-initiiertes iSCSI** – Der ESX Server 3-Host verbindet sich über einen iSCSI-HBA eines anderen Anbieters mit einem Speicher.
- **Software-initiiertes iSCSI** – Der ESX Server 3-Host verwendet einen auf Software basierenden iSCSI-Initiator im VMkernel für die Verbindung zum Speicher. Bei diesem iSCSI-Verbindungstyp benötigt der Host nur einen Standardnetzwerkadapter zum Herstellen der Netzwerkverbindung.

- **NAS (Network-Attached Storage, über das Netzwerk angebundener Speicher)** – Speichert Dateien virtueller Maschinen auf externen Dateiservern, auf die über ein standardmäßiges TCP/IP-Netzwerk zugegriffen wird. Der in ESX Server 3 integrierte NFS-Client verwendet das NFS-Protokoll Version 3 (Network File System), um mit den NAS-/NFS-Servern zu kommunizieren. Für die Netzwerkverbindung benötigt der ESX Server 3-Host einen Standardnetzwerkadapter.

Siehe *Handbuch zur SAN-/Speicherkompatibilität* unter www.vmware.com/pdf/vi3_san_guide.pdf.

Unterstützte Speicheradapter

Für den Zugriff auf verschiedene Speichertypen benötigt das ESX Server 3-System ggf. verschiedene Adapter, um eine Verbindung zum Speichergerät oder Netzwerk aufbauen zu können. ESX Server 3 unterstützt mit SCSI, iSCSI, RAID, Fibre-Channel und Ethernet verschiedene Adapterklassen. ESX Server 3 greift auf die Adapter direkt über Gerätetreiber im VMkernel zu.

Informationen zu von ESX Server 3 unterstützten Adaptertypen finden Sie im *Handbuch zur E/A-Kompatibilität* unter www.vmware.com/support/pubs/vi_pubs.html.

Datenspeicher

Mit dem VI-Client greifen Sie auf verschiedene Arten von Speichergeräten zu, die der ESX Server 3-Host erkennt, um darauf Datenspeicher bereitzustellen. Datenspeicher sind besondere logische Container (analog zu Dateisystemen), bei denen Angaben zu den einzelnen Speichergeräten verborgen bleiben und die ein einheitliches Modell für die Speicherung der Dateien virtueller Maschinen bieten.

Datenspeicher können auch zum Speichern von ISO-Images, Vorlagen virtueller Maschinen und Disketten-Images genutzt werden. Siehe *Grundlagen der Systemverwaltung* unter www.vmware.com/support/pubs/.

Je nach Typ des verwendeten Speichers können ESX Server 3-Datenspeicher die folgenden Dateisystemformate aufweisen:

- **VMFS (Virtual Machine File System)** – Ein spezielles Hochleistungsdateisystem für die Speicherung virtueller ESX Server 3-Maschinen. VMFS kann von ESX Server 3 auf verschiedenen SCSI-basierten lokalen oder Netzwerkspeichergeräten bereitgestellt werden, u. a. auf Fibre-Channel- und iSCSI-SAN-Systemen.

  Als Alternative zur Verwendung eines VMFS-Datenspeichers kann Ihre virtuelle Maschine über eine Zuordnungsdatei (RDM) als Stellvertreter direkt auf Raw-Geräte zugreifen. Weitere Informationen über Raw-Gerätezuordnungen finden Sie unter „Raw-Gerätezuordnung“ auf Seite 155.

- **NFS (Network File System, Netzwerkdateisystem)** – Ein Dateisystem auf einem NAS-Speichergerät. ESX Server 3 unterstützt NFS, Version 3, über TCP/IP. ESX Server 3 kann auf ein angegebenes NFS-Volume auf einem NFS-Server zugreifen. ESX Server 3 mountet das NFS-Volume und nutzt es für Speicherzwecke.

Wenn Sie über die Servicekonsole auf den ESX Server 3-Host zugreifen, werden die VMFS- und NFS-Datenspeicher als getrennte Unterverzeichnisse im Verzeichnis `/vmfs/volumes` angezeigt. Informationen zur Verwendung der Befehle und Dienstprogramme der Servicekonsole finden Sie unter „Verwenden von „vmkfstools““ auf Seite 299.

VMFS-Datenspeicher

Wenn der ESX Server 3-Host auf SCSI-basierte Speichergeräte wie SCSI-, iSCSI- oder FC-SAN zugreift, wird der Speicherplatz ESX Server 3 als LUN angezeigt. Eine *LUN* ist ein logisches Volume, das Speicherplatz auf einer einzelnen physischen Festplatte oder auf einer Vielzahl von Festplatten in einem Festplattenarray anzeigt. Eine einzelne LUN kann aus dem gesamten Speicherplatz auf der Speicherfestplatte bzw. im Array bzw. aus einem Teil des Speicherplatzes erstellt werden, der *Partition* genannt wird. Die LUN, die Festplattenspeicher auf mehreren physischen Festplatten oder Partitionen belegt, wird auf dem ESX Server 3-Host weiterhin als ein logisches Volume angezeigt.

ESX Server 3 kann LUNs als VMFS-Datenspeicher formatieren. VMFS-Datenspeicher dienen hauptsächlich als Ablagen für virtuelle Maschinen. Sie können mehrere virtuelle Maschinen auf demselben VMFS-Volume speichern. Jede virtuelle Maschine ist in einem Satz Dateien gekapselt und belegt ein eigenes Verzeichnis. Für das Betriebssystem innerhalb der virtuellen Maschine behält VMFS die interne Dateisystemsemantik bei. Dadurch wird das ordnungsgemäße Verhalten von Anwendungen und die Datensicherheit für Anwendungen gewährleistet, die in virtuellen Maschinen ausgeführt werden.

Darüber hinaus können Sie in VMFS-Datenspeichern andere Dateien speichern, z. B. Vorlagen virtueller Maschinen und ISO-Images.

VMFS unterstützt die folgenden Datei- und Blockgrößen, sodass Sie auch die datenhungrigsten Anwendungen wie Datenbanken, ERP und CRM in virtuellen Maschinen ausführen können:

- Maximale Größe der virtuellen Festplatte: 2 TB mit einer Blockgröße von 8 MB
- Maximale Dateigröße: 2 TB mit einer Blockgröße von 8 MB
- Blockgröße: 1 MB (Standard), 2 MB, 4 MB und 8 MB

Erstellen und Vergrößern von VMFS-Datenspeichern

Mit dem VI-Client können Sie einen VMFS-Datenspeicher im Vorfeld auf allen SCSI-basierten Speichergeräten einrichten, die Ihr ESX Server 3 erkennt. Mit ESX Server 3 können Sie bis zu 256 VMFS-Datenspeicher pro System bei einer Volume-Mindestgröße von 1,2 GB verwenden.

HINWEIS Ordnen Sie jeder LUN stets nur einen VMFS-Datenspeicher zu.

Informationen zum Erstellen von VMFS-Datenspeichern auf SCSI-basierten Speichergeräten finden Sie in den folgenden Abschnitten:

- „Hinzufügen von lokalem Speicher“ auf Seite 110
- „Hinzufügen von Fibre-Channel-Speicher“ auf Seite 114
- „Hinzufügen von iSCSI-Speicher, auf den über Hardware-Initiatoren zugegriffen werden kann“ auf Seite 125

Nachdem Sie den VMFS-Datenspeicher erstellt haben, können Sie seine Eigenschaften bearbeiten. Siehe „Bearbeiten von VMFS-Datenspeichern“ auf Seite 143.

Wenn Ihr VMFS-Datenspeicher mehr Speicherplatz benötigt, können Sie durch Hinzufügen einer Erweiterung das VMFS-Volume auf bis zu 64 TB dynamisch vergrößern. Eine *Erweiterung* ist eine LUN auf einem physischen Speichergerät, die einem vorhandenen VMFS-Datenspeicher dynamisch hinzugefügt werden kann. Der Datenspeicher kann sich über mehrere Erweiterungen erstrecken und wird dennoch als einzelnes Volume angezeigt.

HINWEIS Sie können kein VMFS-Volume neu formatieren, das ein ESX Server -Remotehost verwendet. Falls Sie es dennoch versuchen, wird eine entsprechende Warnung eingeblendet, in welcher der Name des verwendeten Volumes und die MAC-Adresse einer Hostnetzwerkkarte angegeben sind, die diese verwendet. Diese Warnung wird auch im VMkernel und in **vmkwarning** Protokolldateien angezeigt.

Aspekte beim Erstellen von VMFS-Datenspeichern

Bevor Sie Speichergeräte mit einem VMFS-Datenspeicher formatieren, müssen Sie zunächst festlegen, wie Sie den Speicher für Ihre ESX Server 3-Systeme einrichten wollen.

Die folgenden Gründe sprechen für weniger und dafür größere VMFS-Volumes:

- Mehr Flexibilität beim Erstellen virtueller Maschinen, ohne beim Speicheradministrator mehr Speicherplatz anfordern zu müssen.
- Mehr Flexibilität bei der Größenänderung virtueller Festplatten, dem Erstellen von Snapshots usw.
- Weniger zu verwaltende VMFS-Datenspeicher.

Die folgenden Gründe sprechen für mehr und dafür kleinere VMFS-Volumes:

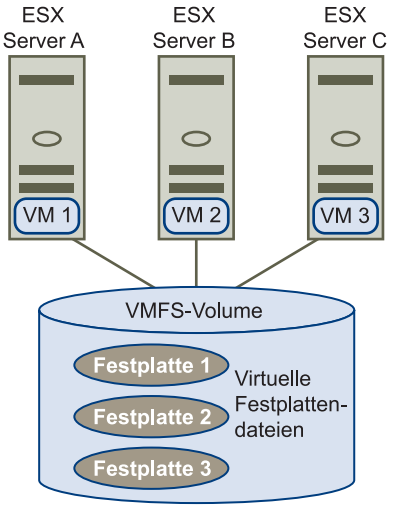
- Weniger falsch genutzter Speicherplatz.
- Unterschiedliche Anwendungen könnten unterschiedliche RAID-Merkmale erfordern.
- Mehr Flexibilität, da die Multipathing-Richtlinie und gemeinsam genutzte Festplattenfreigaben pro LUN festgelegt werden.
- Für den Einsatz von Microsoft Clusterdienst muss jede Clusterfestplattenressource in ihrer eigenen LUN eingerichtet sein.
- Bessere Leistung.

Unter Umständen kann es sinnvoll sein, einige Ihrer Server für wenige, größere VMFS-Volumes zu konfigurieren und andere für mehr und kleinere VMFS-Volumes.

Gemeinsames Nutzen eines VMFS-Volumes durch mehrere ESX Server 3-Systeme

Als Clusterdateisystem ermöglicht VMFS mehreren ESX Server 3-Hosts, parallel auf denselben VMFS-Datenspeicher zuzugreifen. Sie können bis zu 32 Hosts mit einem einzelnen VMFS-Volume verbinden.

Abbildung 5-1. Gemeinsames Nutzen eines VMFS-Volumes durch mehrere ESX Server 3-Hosts



Um zu gewährleisten, dass nicht mehrere Server gleichzeitig auf dieselbe virtuelle Maschine zugreifen, verfügt VMFS über eine festplatteninterne Sperrung.

Die gemeinsame Nutzung desselben VMFS-Volumes durch mehrere ESX Server 3-Hosts bietet Ihnen die folgenden Vorteile:

- Sie können VMware Distributed Resource Scheduling und VMware High Availability einsetzen.

  Sie können virtuelle Maschinen auf mehrere physische Server verteilen. Sie können also auf jedem Server eine Kombination virtueller Maschinen ausführen, sodass nicht alle zur selben Zeit im selben Bereich einer hohen Nachfrage unterliegen.

  Falls ein Server ausfällt, können Sie die virtuellen Maschinen auf einem anderen physischen Server neu starten. Im Störfall wird die festplatteninterne Sperre für die einzelnen virtuellen Maschinen aufgehoben.

  Weitere Informationen zu VMware DRS und VMware HA finden Sie im *Handbuch zur Ressourcenverwaltung* unter www.vmware.com/support/pubs/.

- Mit VMotion können Sie während des laufenden Systembetriebs Migrationen virtueller Maschinen von einem physischen Server auf einen anderen durchführen.

  Weitere Informationen zu VMotion finden Sie in *Grundlagen der Systemverwaltung* unter www.vmware.com/support/pubs/.

- Mit VMware Consolidated Backup kann ein VCB-Proxy genannter Proxy-Server einen Snapshot einer virtuellen Maschine sichern, während diese eingeschaltet ist und Daten in ihren Speicher schreibt und in diesem liest.

  Weitere Informationen zu VMware Consolidated Backup finden Sie im *Sicherungshandbuch für virtuelle Maschinen* unter www.vmware.com/support/pubs/.

NFS-Datenspeicher

ESX Server 3 kann auf ein ausgewähltes NFS-Volume auf einem NAS-Server zugreifen, dieses Volume mounten und es für Speicherzwecke nutzen. Mithilfe von NFS-Volumes können Sie virtuelle Maschinen ebenso wie mithilfe von VMFS-Datenspeichern speichern und starten.

ESX Server unterstützt auf NFS-Volumes die folgenden Funktionen zur gemeinsamen Speichernutzung:

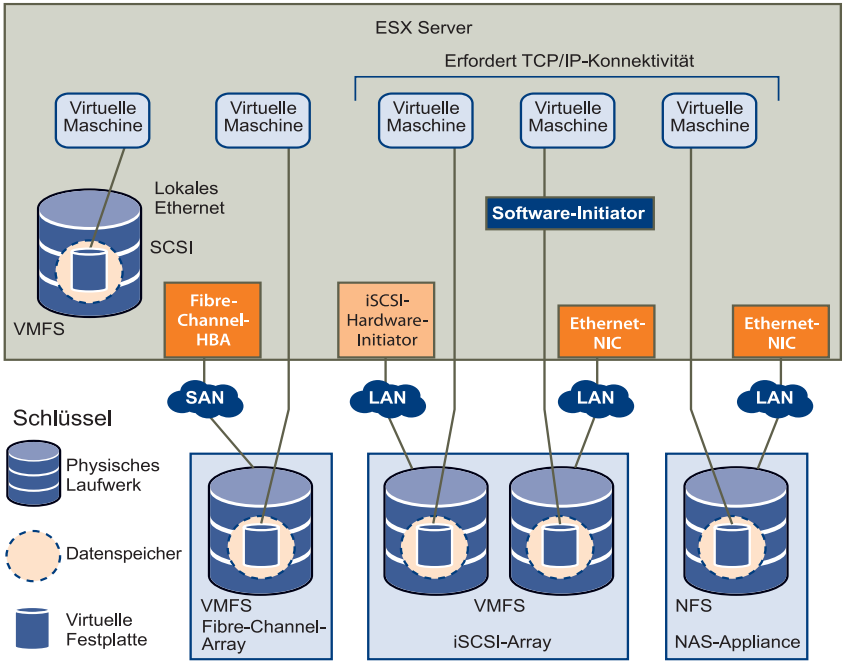
- Verwendung von VMotion.
- Verwendung von VMware DRS and VMware HA.
- Mounten von ISO-Images, die virtuellen Maschinen als CD-ROMs angezeigt werden.
- Erstellung von Snapshots virtueller Maschinen. Siehe *Grundlagen der Systemverwaltung* unter www.vmware.com/support/pubs/.

Speicherzugriff durch virtuelle Maschinen

Wenn eine virtuelle Maschine mit ihrer virtuellen Festplatte kommuniziert, die in einem Datenspeicher gespeichert sind, ruft sie SCSI-Befehle auf. Da sich die Datenspeicher auf verschiedenen Arten physischer Speicher befinden können, werden diese Befehle je nach Protokoll, das das ESX Server 3-System zur Anbindung an ein Speichergerät verwendet, umgewandelt. ESX Server 3 unterstützt die Protokolle Fibre-Channel (FC), Internet-SCSI (iSCSI) und NFS. Unabhängig vom Typ des Speichergeräts, den ESX Server 3 verwendet, wird die virtuelle Festplatte der virtuellen Maschine stets als gemountetes SCSI-Gerät angezeigt. Die virtuelle Festplatte verbirgt die physische Speicherebene vor dem Betriebssystem der virtuellen Maschine. Dadurch können in der virtuellen Maschine auch Betriebssysteme ausgeführt werden, die nicht für bestimmte Speichersysteme, z. B. SAN, zertifiziert sind.

Abbildung 5-2 zeigt die Unterschiede zwischen den Speichertypen: Fünf virtuelle Maschinen verwenden unterschiedliche Arten von Speichern.

Abbildung 5-2. Virtuelle Maschinen mit Zugriff auf verschiedene Speichertypen



HINWEIS Diese Abbildung dient nur zur Veranschaulichung. Es handelt sich nicht um eine empfohlene Konfiguration.

Vergleich der Speichertypen

In Tabelle 5-1 werden die Netzwerkspeichertechnologien verglichen, die ESX Server 3 unterstützt.

Tabelle 5-1. Von ESX Server 3 unterstützter Netzwerkspeicher

Technologie	Protokolle	Übertragungen	Schnittstelle
Fibre-Channel	FC/SCSI	Blockzugriff für Daten/LUN	FC-HBA
iSCSI	IP/SCSI	Blockzugriff für Daten/LUN	■ iSCSI-HBA (Hardware-initiiertes iSCSI) ■ Netzwerkkarte (Software-initiiertes iSCSI)
NAS	IP/NFS	Datei (kein direkter LUN-Zugriff)	Netzwerkkarte

In Tabelle 5-2 werden die ESX Server 3-Funktionen verglichen, welche die verschiedenen Speichertypen unterstützen.

Tabelle 5-2. Von Speichertypen unterstützte ESX Server 3-Funktionen

Speichertyp	Starten von VMs	VMotion	Datenspeicher	Raw-Gerätezuordnung	VM-Cluster	VMware HA und DRS	VCB
SCSI	Ja	Nein	VMFS	Nein	Nein	Nein	Ja
Fibre-Channel	Ja	Ja	VMFS	Ja	Ja	Ja	Ja
iSCSI	Ja	Ja	VMFS	Ja	Nein	Ja	Ja
NAS über NFS	Ja	Ja	NFS	Nein	Nein	Ja	Ja

Anzeigen der Speicherinformationen im VMware Infrastructure-Client

Der VI-Client zeigt detaillierte Informationen über verfügbare Datenspeicher, Speichergeräte, die von den Datenspeichern verwendet werden, und die Adapterkonfiguration an. Weitere Informationen finden Sie in folgenden Abschnitten:

- „Anzeigen von Datenspeichern“ auf Seite 103
- „Anzeigen von Speicheradaptern“ auf Seite 104
- „Grundlegendes zur Benennung von Speichergeräten in der Anzeige“ auf Seite 105

Anzeigen von Datenspeichern

Es gibt folgende Möglichkeiten, dem VI-Client Datenspeicher hinzufügen:

- Erkennung, sobald ein Host der Bestandsliste hinzugefügt wird. Wenn Sie der Bestandsliste einen Host hinzufügen, zeigt der VI-Client alle Datenspeicher an, die dem Host zur Verfügung stehen.
- Erstellung auf einem verfügbaren Speichergerät. Über den Befehl **Speicher hinzufügen (Add Storage)** können Sie einen neuen Datenspeicher erstellen und konfigurieren. Siehe „Speicherkonfiguration“ auf Seite 109.

Sie können ein Verzeichnis der verfügbaren Datenspeicher anzeigen und ihre Eigenschaften analysieren.

Um Datenspeicher anzuzeigen, klicken Sie auf dem Host auf der Registerkarte **Konfiguration (Configuration)** auf **Speicher (Storage)**.

Der Abschnitt **Speicher (Storage)** zeigt für jede Datenbank eine Übersicht an. Hier sind folgende Daten zu finden:

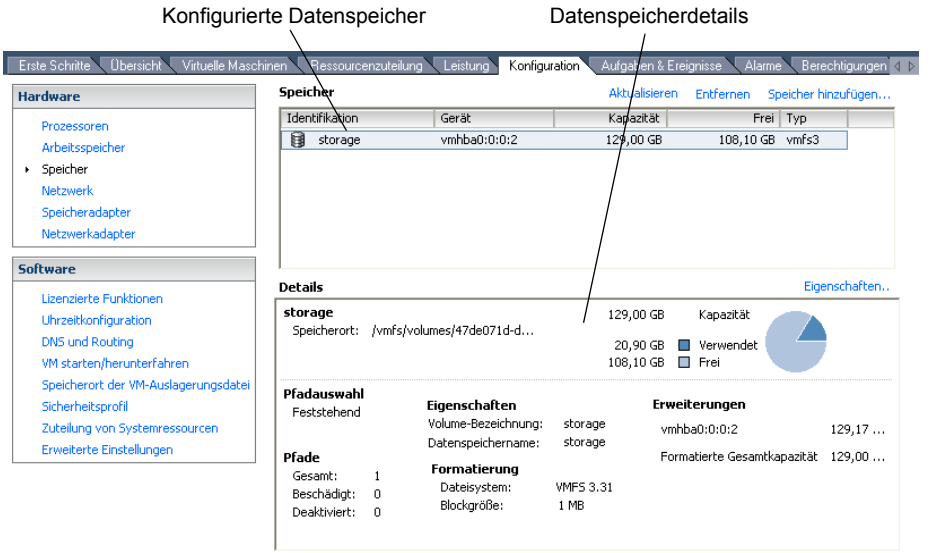
- Das Zielspeichergerät, auf dem sich der Datenspeicher befindet. Siehe „Grundlegendes zur Benennung von Speichergeräten in der Anzeige“ auf Seite 105.
- Die Art des Dateisystems, das der Datenspeicher verwendet. Siehe „Datenspeicher“ auf Seite 95.
- Die Gesamtkapazität sowie der belegte und freie Speicher.

Wählen Sie den Datenspeicher in der Liste aus, wenn Sie zusätzlich Details erfahren möchten. Der Abschnitt **Details** enthält folgende Informationen:

- Den Speicherort des Datenspeichers
- Einzelne Erweiterungen, aus denen der Datenspeicher besteht, samt Kapazität (VMFS-Datenspeicher)
- Pfade, die zum Zugriff auf das Speichergerät verwendet werden (VMFS-Datenspeicher)

In Abbildung 5-3 wurde der Datenspeicher **symm-07** in der Liste der verfügbaren Datenspeicher ausgewählt. Der Bereich **Details** zeigt Informationen zum ausgewählten Datenspeicher.

Abbildung 5-3. Informationen zu Datenspeichern



Sie können vorhandene Datenspeicher aktualisieren und entfernen sowie die Eigenschaften eines VMFS-Datenspeichers ändern. Bei der Bearbeitung oder Neukonfiguration eines VMFS-Datenspeichers können Sie seine Bezeichnung ändern, ihn aktualisieren, Erweiterungen hinzufügen oder Pfade zu Speichergeräten ändern. Siehe „Speicherverwaltung“ auf Seite 141.

Anzeigen von Speicheradaptern

Der VI-Client zeigt alle Speicheradapter an, die im System zur Verfügung stehen.

Um Speicheradapter anzuzeigen, klicken Sie auf dem Host auf der Registerkarte **Konfiguration (Configuration)** auf **Speicheradapter (Storage Adapters)**.

Sie können zu Speicheradaptern die folgenden Informationen anzeigen:

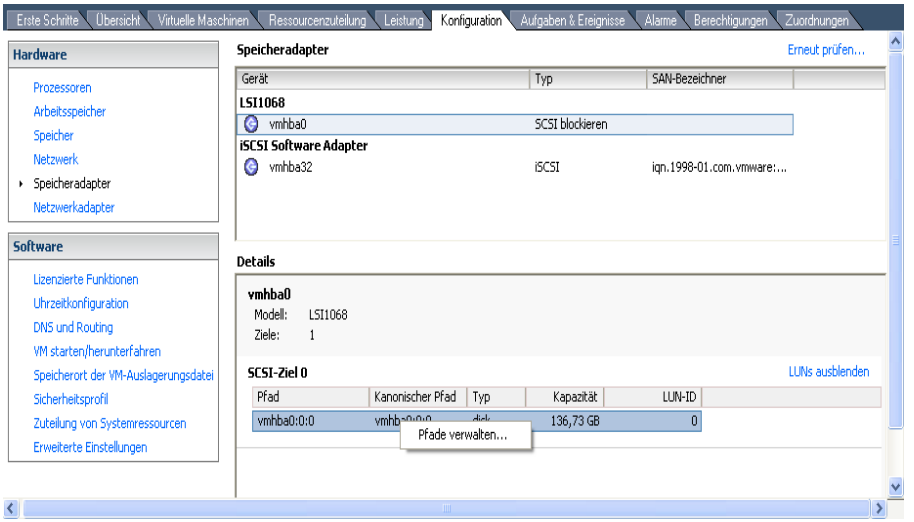
- Vorhandene Speicheradapter.
- Art des Speicheradapters, z. B. Fibre-Channel, SCSI oder iSCSI.
- Details zu jedem Adapter, z. B. das angebundene Speichergerät und die Ziel-ID.

Um die Konfigurationseigenschaften eines bestimmten Adapters anzuzeigen, markieren Sie den Adapter in der Liste **Speicheradapter (Storage Adapters)**.

In Abbildung 5-4 ist der iSCSI-Hardware-Adapter „vmhba0“ markiert. Der Bereich **Details** gibt Auskunft über die Anzahl der LUNs, an die der Adapter angebunden ist, und über die verwendeten Pfade.

Um die Konfiguration des Pfades zu ändern, markieren Sie den Pfad in der Liste, klicken mit der rechten Maustaste auf den Pfad und klicken auf **Pfade verwalten (Manage Paths)**. Das Dialogfeld **Pfade verwalten (Manage Paths)** wird geöffnet. Siehe „Verwalten mehrerer Pfade“ auf Seite 146.

Abbildung 5-4. Informationen zu Speicheradaptern



Grundlegendes zur Benennung von Speichergeräten in der Anzeige

Im VI-Client wird der Name eines Speichergeräts als Abfolge von drei oder vier Zahlen angegeben, die durch Doppelpunkte getrennt sind, z. B. `vmhba1:1:3:1`. Dieser Name hat die folgende Bedeutung:

`<HBA>:<SCSI-Ziel>:<SCSI-LUN>:<Festplattenpartition>`

Die Abkürzung `vmhba` bezieht sich auf verschiedene physische HBAs im ESX Server 3-System. Sie kann sich auch auf den virtuellen iSCSI-Initiator beziehen, den ESX Server 3 unter Verwendung des VMkernel-Netzwerkstapels implementiert. Die vierte Zahl gibt eine Partition auf einer Festplatte an, die ein VMFS-Datenspeicher belegt.

Das Beispiel `vmhba1:1:3:1` bezieht sich auf die erste Partition auf SCSI-LUN 3, SCSI-Ziel 1, auf die über HBA 1 zugegriffen wird.

Die dritte und vierte Zahl ändern sich nie, die ersten beiden Zahlen können sich jedoch ändern. Beispielsweise kann sich nach einem Neustart des ESX Server 3-Systems `vmhba1:1:3:1` in `vmhba3:2:3:1` ändern. Der Name bezieht sich jedoch immer noch auf dasselbe physische Gerät. Die erste und zweite Zahl können sich aus den folgenden Gründen ändern:

- Die erste Zahl, der HBA, ändert sich, wenn im Fibre-Channel- oder iSCSI-Netzwerk ein Ausfall auftritt. In diesem Fall muss das ESX Server 3-System für den Zugriff auf das Speichergerät einen anderen HBA verwenden.
- Die zweite Zahl, das SCSI-Ziel, ändert sich bei Änderungen der Zuordnungen der Fibre-Channel- oder iSCSI-Ziele, die für den ESX Server 3-Host sichtbar sind.

Konfigurieren und Verwalten von Speichern

Die Kapitel zum Konfigurieren und Verwalten des Speichers in diesem Handbuch behandeln die wichtigsten Konzepte und Aufgaben, die bei der Arbeit mit Speichern erforderlich sind.

Weitere Informationen zum Konfigurieren von SANs finden Sie im *SAN-Konfigurationshandbuch (für Fiber Channel)* und im *SAN-Konfigurationshandbuch (für iSCSI)*.

Weitere Informationen zu bestimmten Speicherkonfigurationsaufgaben finden Sie unter folgenden Themen:

- Konfiguration von lokalem Speicher:

  „So erstellen Sie einen Datenspeicher auf einer lokalen SCSI-Festplatte“ auf Seite 111

- Konfiguration von Fibre-Channel-SAN-Speicher:

  „So erstellen Sie einen Datenspeicher auf einem Fibre-Channel-Gerät“ auf Seite 114

- Konfiguration von Hardware-initiiertem iSCSI-Speicher:
  - „So zeigen Sie die Eigenschaften des Hardware-iSCSI-Initiators an“ auf Seite 119
  - „So konfigurieren Sie den iSCSI-Namen, Alias und die IP-Adresse für den Hardware-Initiator“ auf Seite 121
  - „So richten Sie Zielerkennungsadressen mithilfe der dynamischen Erkennung ein“ auf Seite 122
  - „So richten Sie CHAP-Parameter für den Hardware-Initiator ein“ auf Seite 124
  - „So erstellen Sie einen Datenspeicher auf einem Hardware-iSCSI-Gerät“ auf Seite 125

- Konfiguration von Software-initiiertem iSCSI-Speicher:
  - „So zeigen Sie die Eigenschaften des Software-iSCSI-Initiators an“ auf Seite 128
  - „So aktivieren Sie den Software-iSCSI-Initiator“ auf Seite 130
  - „So richten Sie Zielerkennungsadressen für den Software-Initiator ein“ auf Seite 130
  - „So richten Sie CHAP-Parameter für den Software-Initiator ein“ auf Seite 131
  - „So erstellen Sie einen Datenspeicher auf einem iSCSI-Gerät, auf das über Software-Initiatoren zugegriffen wird“ auf Seite 132
- Konfiguration von NAS-Speicher:

  „So mounten Sie ein NFS-Volume“ auf Seite 137
- Speicherverwaltung:
  - „So aktualisieren Sie VMFS-2 in VMFS-3“ auf Seite 144
  - „So ändern Sie den Namen des Datenspeichers“ auf Seite 144
  - „So fügen Sie Erweiterungen einem Datenspeicher hinzu“ auf Seite 145
  - „So entfernen Sie einen Datenspeicher“ auf Seite 143
- Pfadverwaltung:
  - „So richten Sie die Multipathing-Richtlinie ein“ auf Seite 152
  - „So richten Sie den bevorzugten Pfad ein“ auf Seite 153
  - „So deaktivieren Sie einen Pfad“ auf Seite 153

Speicherkonfiguration 6

Dieses Kapitel enthält Informationen zur Konfiguration lokaler SCSI-Speichergeräte sowie zur Fibre-Channel-SAN-, iSCSI- und NAS-Speicherung.

HINWEIS Weitere Informationen zum Konfigurieren von SANs finden Sie im *SAN-Konfigurationshandbuch (für Fiber Channel)* und im *SAN-Konfigurationshandbuch (für iSCSI)*.

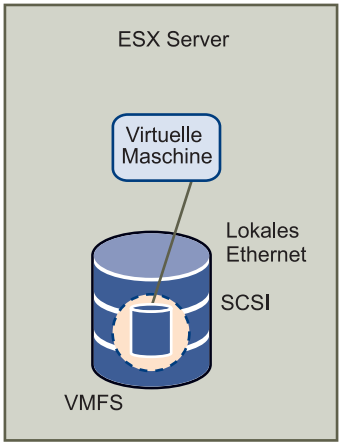
In diesem Kapitel werden folgende Themen behandelt:

- „Lokaler Speicher“ auf Seite 110
- „Fibre-Channel-Speicher“ auf Seite 113
- „iSCSI-Speicher“ auf Seite 116
- „Starten einer erneuten Prüfung“ auf Seite 134
- „Network Attached Storage (NAS)“ auf Seite 135
- „Erstellen einer Diagnosepartition“ auf Seite 138

Lokaler Speicher

Der lokale Speicher verwendet ein SCSI-Gerät, wie z. B. die Festplatte des ESX Server 3-Hosts oder ein externes dediziertes Speichersystem, das direkt an den ESX Server 3-Host angeschlossen ist. Abbildung 6-1 zeigt eine virtuelle Maschine, die einen lokalen SCSI-Speicher verwendet.

Abbildung 6-1. Lokaler Speicher



Bei diesem Beispiel einer lokalen Speichertopologie verwendet der ESX Server 3-Host eine einzelne Verbindung, um eine Festplatte anzuschließen. Auf dieser Festplatte können Sie einen VMFS-Datenspeicher erstellen, der zur Speicherung der Festplattendateien der virtuellen Maschine verwendet wird.

Wenngleich diese Speicherkonfiguration möglich ist, wird sie nicht empfohlen. Das Verwenden einzelner Verbindungen zwischen Speicherarrays und ESX Server 3-Hosts sorgt für *einzelne Ausfallstellen*, die Störungen verursachen können, wenn eine Verbindung unzuverlässig wird oder ausfällt. Um für Fehlertoleranz zu sorgen, unterstützen verschiedene direkt angeschlossene Speichersysteme redundante Verbindungspfade. Siehe „Verwalten mehrerer Pfade“ auf Seite 146.

Hinzufügen von lokalem Speicher

Beim Laden der Treiber für die SCSI-Speicheradapter erkennt ESX Server 3 die verfügbaren SCSI-Speichergeräte. Bevor Sie einen neuen Datenspeicher auf einem SCSI-Gerät erstellen, müssen Sie ggf. erneut nach Speichergeräten suchen. Siehe „Starten einer erneuten Prüfung“ auf Seite 134.

Wenn Sie einen Datenspeicher auf einem SCSI-Speichergerät erstellen, führt Sie der Assistent zum Hinzufügen von Speicher durch die Konfiguration.

So erstellen Sie einen Datenspeicher auf einer lokalen SCSI-Festplatte

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend unter **Hardware** auf **Speicher (Storage)**.

3 Klicken Sie auf **Speicher hinzufügen (Add Storage)**.

4 Markieren Sie den Speichertyp **Festplatte/LUN (Disk/LUN)**, und klicken Sie auf **Weiter (Next)**.

5 Wählen Sie das SCSI-Gerät aus, das Sie für den Datenspeicher verwenden möchten, und klicken Sie auf **Weiter (Next)**.

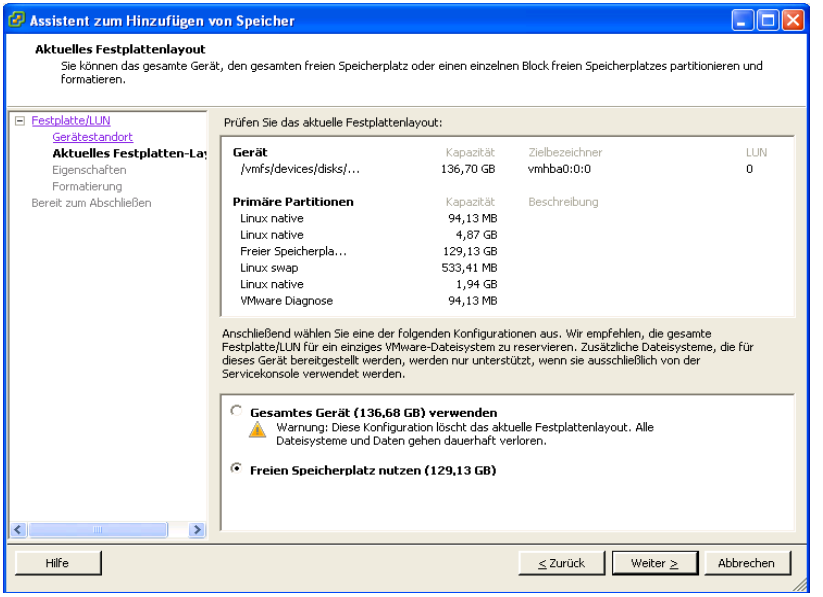
   Die Seite **Aktuelles Festplattenlayout (Current Disk Layout)** wird angezeigt. Wenn die zu formatierende Festplatte leer ist, zeigt die Seite **Aktuelles Festplattenlayout (Current Disk Layout)** automatisch den gesamten Speicherplatz der Festplatte, der für die Konfiguration zur Verfügung steht.

6 Wenn die Festplatte nicht leer ist, überprüfen Sie im oberen Bereich auf der Seite **Aktuelles Festplattenlayout (Current Disk Layout)** das aktuelles Festplattenlayout, und wählen Sie im unteren Bereich eine Konfigurationsoption aus:

   - **Gesamtes Gerät verwenden (Use the entire device)** – Wählen Sie diese Option, um die gesamte Festplatte oder LUN einem einzelnen VMFS-Datenspeicher zur Verfügung zu stellen. VMware empfiehlt das Aktivieren dieser Option.

WARNUNG Bei Wahl dieser Option werden zuvor auf diesem Gerät gespeicherte Dateisysteme und Daten dauerhaft gelöscht.

- **Freien Speicherplatz verwenden (Use free space)** – Wählen Sie diese Option, um einen VMFS-Datenspeicher im verbleibenden freien Speicherplatz auf der Festplatte bereitzustellen.



7 Klicken Sie auf **Weiter (Next)**.

8 Geben Sie auf der Seite **Festplatte/LUN–Eigenschaften (Disk/LUN–Properties)** einen Dateispeichernamen ein, und klicken Sie auf **Weiter (Next)**.

Die Seite **Festplatte/LUN–Formatierung (Disk/LUN–Formatting)** wird angezeigt.

9 Passen Sie bei Bedarf das Dateisystem und die Größen an.

Standardmäßig wird der gesamte freie Speicherplatz des Speichergeräts angeboten.

10 Klicken Sie auf **Weiter (Next)**.

11 Überprüfen Sie im Fenster **Fertig zur Weiterbearbeitung (Ready to Complete)** die Informationen zur Datenspeicherkonfiguration, und klicken Sie auf **Fertig (Finish)**.

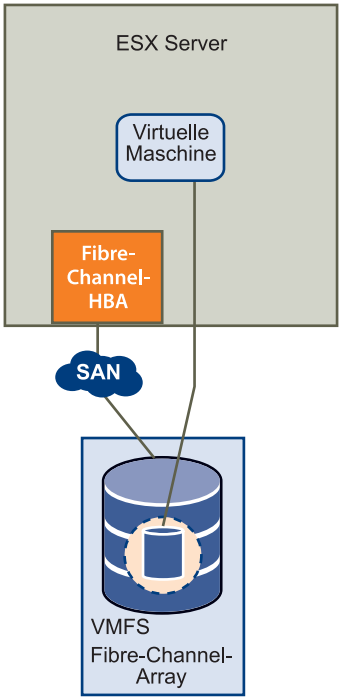
Durch diesen Prozess wird ein Datenspeicher auf einer lokalen SCSI-Festplatte auf Ihrem ESX Server 3-Host erstellt.

Fibre-Channel-Speicher

ESX Server 3 unterstützt Fibre-Channel-Adapter, über die ein ESX Server 3-System an ein SAN angebunden werden kann und somit in der Lage ist, die Festplatten-Arrays im SAN zu erkennen.

Abbildung 6-2 zeigt virtuelle Maschinen, die einen Fibre-Channel-Speicher verwenden.

Abbildung 6-2. Fibre-Channel-Speicher



Bei dieser Konfiguration ist das ESX Server 3-System mithilfe eines Fibre-Channel-Adapters mit einem SAN-Fabric verbunden, das aus Fibre-Channel-Switches und Speicherarrays besteht. LUNs eines Speicherarrays können nun vom ESX Server 3-System verwendet werden. Sie können auf die LUNs zugreifen und einen Datenspeicher erstellen, der für die Speicheranforderungen von ESX Server 3 verwendet werden kann. Der Datenspeicher verwendet das VMFS-Format.

In den folgenden Dokumenten finden Sie zusätzliche Informationen:

- Siehe „Hinzufügen von Fibre-Channel-Speicher“ auf Seite 114.
- Informationen zur Konfiguration von SANs finden Sie im *SAN-Konfigurationshandbuch (für Fiber Channel)*.

- Informationen zu unterstützten SAN-Speichergeräten für ESX Server 3 finden Sie im *Handbuch zur SAN-/Speicherkompatibilität*.
- Informationen zu Multipathing für Fibre-Channel-HBAs und die Verwaltung von Pfaden finden Sie unter „Verwalten mehrerer Pfade“ auf Seite 146.

Hinzufügen von Fibre-Channel-Speicher

Prüfen Sie den Fibre-Channel-Adapter vor der Erstellung eines neuen Datenspeichers auf einem Fibre-Channel-Gerät erneut, um ggf. neu hinzugefügte LUNs zu erkennen. Siehe „Starten einer erneuten Prüfung“ auf Seite 134.

Wenn Sie einen Datenspeicher auf einem Fibre-Channel-Speichergerät erstellen, führt Sie der Assistent zum Hinzufügen von Speicher durch die Konfiguration.

So erstellen Sie einen Datenspeicher auf einem Fibre-Channel-Gerät

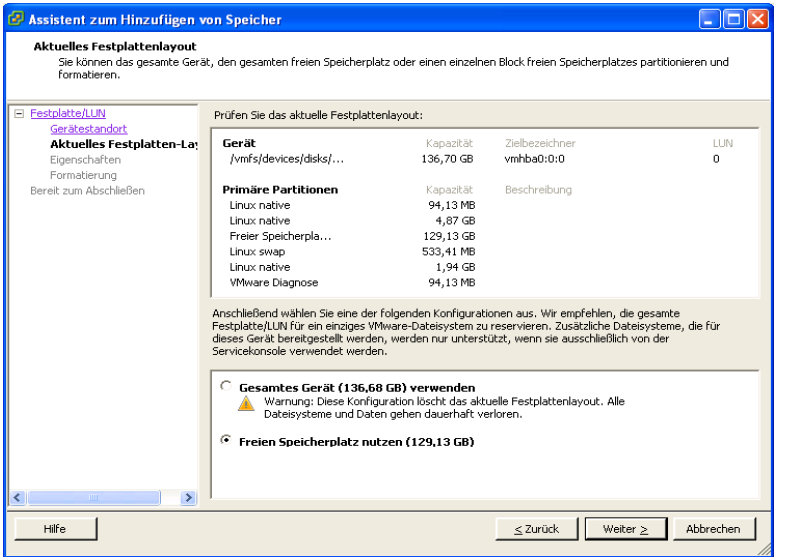
1. Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.
2. Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend unter **Hardware** auf **Speicher (Storage)**.
3. Klicken Sie auf **Speicher hinzufügen (Add Storage)**.
4. Markieren Sie den Speichertyp **Festplatte/LUN (Disk/LUN)**, und klicken Sie auf **Weiter (Next)**.
5. Wählen Sie das Fibre-Channel-Gerät aus, das Sie für den Datenspeicher verwenden möchten, und klicken Sie auf **Weiter (Next)**.

   Die Seite **Aktuelles Festplattenlayout (Current Disk Layout)** wird angezeigt. Wenn die zu formatierende Festplatte leer ist, zeigt die Seite **Aktuelles Festplattenlayout (Current Disk Layout)** automatisch den gesamten Speicherplatz der Festplatte, der für die Konfiguration zur Verfügung steht.
6. Wenn die Festplatte nicht leer ist, überprüfen Sie im oberen Bereich auf der Seite **Aktuelles Festplattenlayout (Current Disk Layout)** das aktuelles Festplattenlayout, und wählen Sie im unteren Bereich eine Konfigurationsoption aus:

   - **Gesamtes Gerät verwenden (Use the entire device)** – Wählen Sie diese Option, um die gesamte Festplatte oder LUN einem einzelnen VMFS-Datenspeicher zur Verfügung zu stellen. VMware empfiehlt das Aktivieren dieser Option.

WARNUNG Bei Wahl dieser Option werden zuvor auf diesem Gerät gespeicherte Dateisysteme und Daten dauerhaft gelöscht.

- **Freien Speicherplatz verwenden (Use free space)** – Wählen Sie diese Option, um einen VMFS-Datenspeicher im verbleibenden freien Speicherplatz auf der Festplatte bereitzustellen.



7 Klicken Sie auf **Weiter (Next)**.

8 Geben Sie auf der Seite **Festplatte/LUN–Eigenschaften (Disk/LUN–Properties)** einen Dateispeichernamen ein, und klicken Sie auf **Weiter (Next)**.

Die Seite **Formatierung von Festplatte/LUN (Disk/LUN–Formatting)** wird angezeigt.

9 Ändern Sie bei Bedarf die Werte für das Dateisystem und die Größe des Datenspeichers.

Standardmäßig wird der gesamte freie Speicherplatz des Speichergeräts zur Verfügung gestellt.

10 Klicken Sie auf **Weiter (Next)**.

11 Überprüfen Sie auf der Seite **Bereit zum Abschließen (Ready to Complete)** die Informationen zur Datenspeicherkonfiguration, und klicken Sie auf **Fertig (Finish)**.

Dieser Prozess erstellt einen Datenspeicher für den ESX Server 3-Host auf einer Fibre-Channel-Festplatte.

12 Klicken Sie auf **Aktualisieren (Refresh)**.

Informationen zur erweiterten Konfiguration, z. B. die Verwendung von Multipathing, Masking und Zoning finden Sie im *SAN-Konfigurationshandbuch (für Fiber Channel)*.

iSCSI-Speicher

ESX Server 3 unterstützt iSCSI-Technologie, die es dem ESX Server 3-System ermöglicht, beim Zugriff auf Remotespeicher ein IP-Netzwerk zu verwenden. Bei iSCSI werden die SCSI-Speicherbefehle, die die virtuelle Maschine ihren virtuellen Festplatten erteilt, in TCP/IP-Protokollpakete umgewandelt und an ein Remotegerät bzw. Ziel übertragen, auf dem die virtuelle Festplatte gespeichert ist. Aus Sicht der virtuellen Maschine wird das Gerät als lokal angeschlossenes SCSI-Laufwerk angezeigt.

iSCSI-Initiatoren

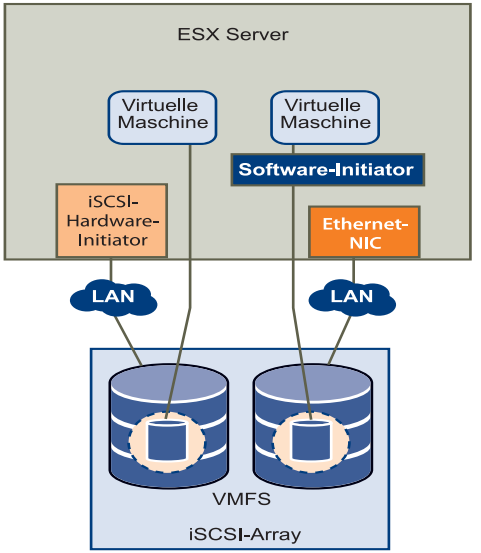
Für den Zugriff auf Remoteziele verwendet der ESX Server 3-Host iSCSI-Initiatoren. Initiatoren übermitteln SCSI-Anforderungen und -Antworten zwischen dem ESX Server 3-System und dem Zielspeichergerät über das IP-Netzwerk.

ESX Server 3 unterstützt hardwarebasierte und softwarebasierte iSCSI-Initiatoren:

- **Hardware-iSCSI-Initiator** – Ein Drittanbieter-HBA (Host Bus Adapter) mit der Funktion „iSCSI über TCP/IP“. Dieser spezielle iSCSI-Adapter ist für die gesamte Verarbeitung und Verwaltung von iSCSI verantwortlich.
- **Software-iSCSI-Initiator** – Ein in den VMkernel integrierter Code, der es ermöglicht, das ESX Server 3-System mit dem iSCSI-Speichergerät über Standardnetzwerkadapter anzubinden. Der Software-Initiator übernimmt iSCSI-Verarbeitung und kommuniziert gleichzeitig über den Netzwerkstapel mit dem Netzwerkadapter. Mit dem Software-Initiator können Sie die iSCSI-Technologie verwenden, ohne besondere Hardware anschaffen zu müssen.

Abbildung 6-3 zeigt zwei virtuelle Maschinen, die verschiedene Arten von iSCSI-Initiatoren verwenden.

Abbildung 6-3. iSCSI-Speicher



Im ersten Beispiel der iSCSI-Speicherkonfiguration verwendet das ESX Server 3-System einen Hardware-iSCSI-Adapter. Dieser spezielle iSCSI-Adapter sendet iSCSI-Pakete über ein LAN an eine Festplatte.

Im zweiten Beispiel verfügt das ESX Server 3-System über einen Software-iSCSI-Initiator. Unter Verwendung des Software-Initiators stellt das ESX Server 3-System die Verbindung zu einem LAN über eine vorhandene Netzwerkkarte her.

Benennungskonventionen

Da SANs sehr groß und komplex werden können, verfügen alle iSCSI-Initiatoren und -Ziele im Netzwerk über eindeutige und dauerhafte iSCSI-Namen. Außerdem werden ihnen Zugriffsadressen zugewiesen. Der iSCSI-Name ermöglicht die ordnungsgemäße Identifizierung eines bestimmten iSCSI-Geräts (Initiator oder Ziel) unabhängig von seinem physischen Standort.

Stellen Sie bei der Konfiguration der iSCSI-Initiatoren sicher, dass die Benennungskonventionen eingehalten werden. Die Initiatoren können folgende Formate verwenden:

- **IQN (iSCSI Qualified Name)** – Kann bis zu 255 Zeichen lang sein und hat das folgende Format:

  `iqn.<Jahr–Monat>.<umgekehrter_Domänenname>:<eindeutiger_Name>`

  wobei `<Jahr–Mo>` für das Jahr und den Monat stehen, in dem Ihr Domänenname registriert wurde, `<umgekehrter_Domänenname>` der offizielle Name Ihrer Domäne in umgekehrter Reihenfolge ist, und `<eindeutiger_Name>` ein beliebiger Name ist, den Sie verwenden möchten, z. B. der Name Ihres Servers.

  Beispiel: `iqn.1998–01.com.mycompany:myserver`.

- **EUI (Extended Unique Identifier, erweiterter eindeutiger Bezeichner)** – Das `eui.`-Präfix des eindeutigen Bezeichners, gefolgt vom Namen mit 16 Zeichen. Der Name umfasst 24 Bit für den von der IEEE zugewiesenen Firmennamen und 40 Bit für eine eindeutige ID, zum Beispiel eine Seriennummer.

  Beispiel: `eui.0123456789ABCDEF`.

Erkennungsmethoden

Um festzustellen, welche Speicherressourcen im Netzwerk für den Zugriff verfügbar sind, verwendet das ESX Server 3-System die folgenden Erkennungsmethoden:

- **Dynamische Erkennung** – Wird auch als „Ziele senden"-Erkennungsmethode bezeichnet. Immer wenn der Initiator einen angegebenen iSCSI-Server kontaktiert, wird eine *Ziele senden*-Anforderung an den Server übermittelt. Der Server liefert als Antwort eine Liste verfügbarer Ziele an den Initiator zurück.
- **Statische Erkennung** – Der Initiator führt keine Erkennungsaufgaben aus, da er im Voraus alle Ziele kennt, die kontaktiert werden, und deren IP-Adressen und Domänennamen für die Kommunikation mit ihnen verwendet.

  Die statische Erkennungsmethode steht nur zur Verfügung, wenn über Hardware-Initiatoren auf den iSCSI-Speicher zugegriffen wird.

iSCSI-Sicherheit

Da iSCSI die IP-Netzwerke zur Anbindung an Remoteziele verwendet, muss die Sicherheit der Verbindung gewährleistet werden. Das IP-Protokoll schützt die Daten, die es übermittelt, nicht selbst und kann auch die Legitimität der Initiatoren, die auf die Ziele im Netzwerk zugreifen, nicht überprüfen. Zur Sicherstellung der Sicherheit in IP-Netzwerken müssen Sie gesonderte Maßnahmen ergreifen.

ESX Server 3 unterstützt das Challenge Handshake Authentication Protocol (CHAP), das die iSCSI-Initiatoren zur Authentifizierung nutzen können. Nach der ersten Verbindung mit dem Ziel durch den Initiator überprüft CHAP die Identität des Initiators und prüft den CHAP-Schlüssel, der von Initiator und Ziel gemeinsam genutzt wird. Das kann während der iSCSI-Sitzung regelmäßig wiederholt werden.

Wenn Sie iSCSI-Initiatoren für Ihr ESX Server 3-System konfigurieren, überprüfen Sie, ob der iSCSI-Speicher CHAP unterstützt. Falls ja, muss das Protokoll für Ihre Initiatoren aktiviert werden. Siehe „Absichern von iSCSI-Speicher“ auf Seite 214.

Konfigurieren von Hardware-iSCSI-Initiatoren und -Speicher

Wenn Ihr ESX Server 3 mit dem iSCSI-Speicher über Hardware-Initiatoren kommuniziert, wird ein spezieller Adapter eines anderen Anbieters verwendet, mit dem Sie über TCP/IP auf den iSCSI-Speicher zuzugreifen können. Dieser iSCSI-Adapter steuert die gesamte iSCSI-Verarbeitung und -Verwaltung für das ESX Server 3-System.

Installieren und konfigurieren Sie den Hardware-iSCSI-Adapter vor der Einrichtung des Datenspeichers auf einem iSCSI-Speichergerät.

Installieren und Anzeigen eines Hardware-iSCSI-Initiators

Informationen zu den unterstützen Adaptern finden Sie im *Handbuch zur E/A-Kompatibilität* auf der VMware-Webseite unter www.vmware.com.

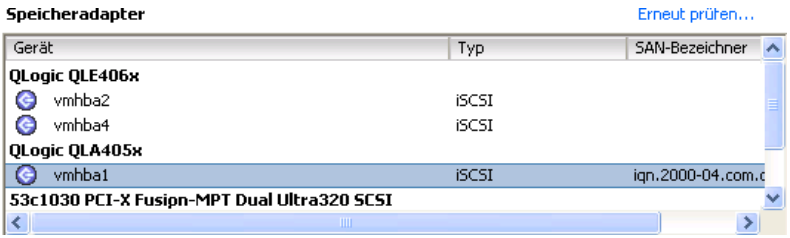
Bevor Sie mit der Konfiguration des Hardware-iSCSI-Initiators beginnen, überprüfen Sie, dass der iSCSI-HBA ordnungsgemäß installiert wurde und in der Liste der konfigurierbaren Adapter angezeigt wird. Wenn der Initiator installiert wurde, können Sie seine Eigenschaften anzeigen.

So zeigen Sie die Eigenschaften des Hardware-iSCSI-Initiators an

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend unter **Hardware** auf **Speicheradapter (Storage Adapters)**.

Der Hardware-iSCSI-Initiator wird in der Liste der Speicheradapter angezeigt.

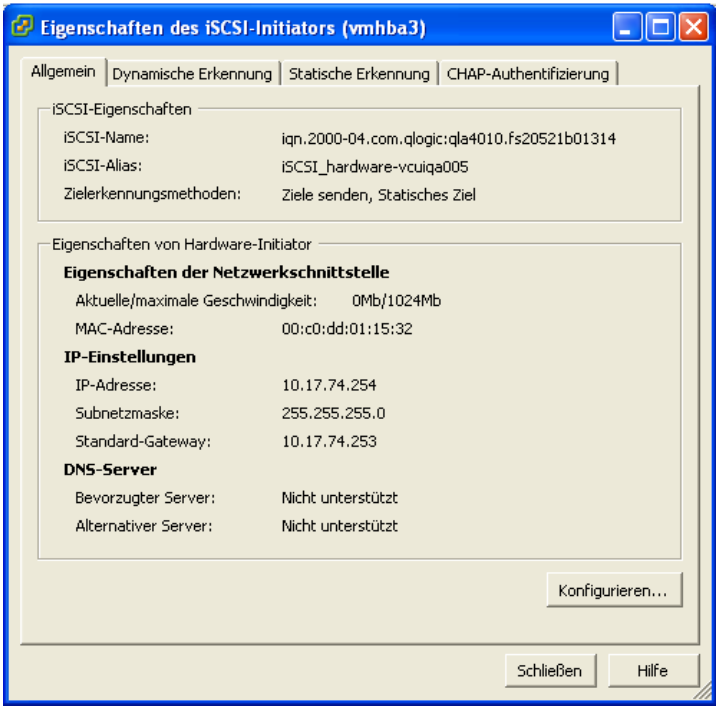


3 Wählen Sie den zu konfigurierenden Initiator aus.

Es werden die Details zu diesem Initiator angezeigt, u. a. Modell, IP-Adresse, iSCSI-Name, Zielerkennung, iSCSI-Alias und erkannte Ziele.

4 Klicken Sie auf **Eigenschaften (Properties)**.

Das Dialogfeld **iSCSI-Initiator-Eigenschaften (iSCSI Initiator Properties)** wird angezeigt. Auf der Registerkarte **Allgemein (General)** werden zusätzliche Merkmale des Initiators angezeigt.



Sie können den Hardware-Initiator jetzt konfigurieren oder seine Standardmerkmale ändern.

Konfiguration eines Hardware-iSCSI-Initiators

Während der Konfiguration des Hardware-iSCSI-Initiators müssen Sie den iSCSI-Namen, die IP-Adresse und die Erkennungsadressen des Initiators einrichten. Darüber hinaus empfiehlt VMware die Einrichtung von CHAP-Parametern.

Nach der Konfiguration des iSCSI-Software-Initiators müssen Sie erneut nach Speichergeräten suchen, damit alle LUNs, auf die der Initiator zugreifen kann, in der Liste der Speichergeräte angezeigt werden. Siehe „Starten einer erneuten Prüfung“ auf Seite 134.

Einrichten von Benennungsparametern

Stellen Sie beim Konfigurieren der Hardware-iSCSI-Initiatoren sicher, dass ihre Namen und IP-Adressen ordnungsgemäß formatiert sind.

Siehe „Benennungskonventionen“ auf Seite 117.

So konfigurieren Sie den iSCSI-Namen, Alias und die IP-Adresse für den Hardware-Initiator

1 Klicken Sie im Dialogfeld **Eigenschaften des iSCSI-Initiators (iSCSI Initiator Properties)** auf die Schaltfläche **Konfigurieren (Configure)**.

2 Um den Standard-iSCSI-Namen für den Initiator zu ändern, geben Sie einen neuen iSCSI-Namen ein.

   Sie können den vom Hersteller angegebenen Standardnamen verwenden. Wenn Sie den Standardnamen ändern möchten, müssen Sie sicherstellen, dass der neue Name ordnungsgemäß formatiert ist. Andernfalls können einige Speichergeräte den Hardware-iSCSI-Initiator ggf. nicht erkennen.

3 Geben Sie den iSCSI-Alias ein.

   Das Alias ist ein Name, der zur Identifizierung des Hardware-iSCSI-Initiators verwendet wird.

4 Geben Sie unter **Eigenschaften von Hardware-Initiator (Hardware Initiator Properties)** alle benötigen Angaben ein.

5 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

6 Starten Sie den Server neu, damit die Änderungen wirksam werden.

Einrichten von Erkennungsadressen für Hardware-Initiatoren

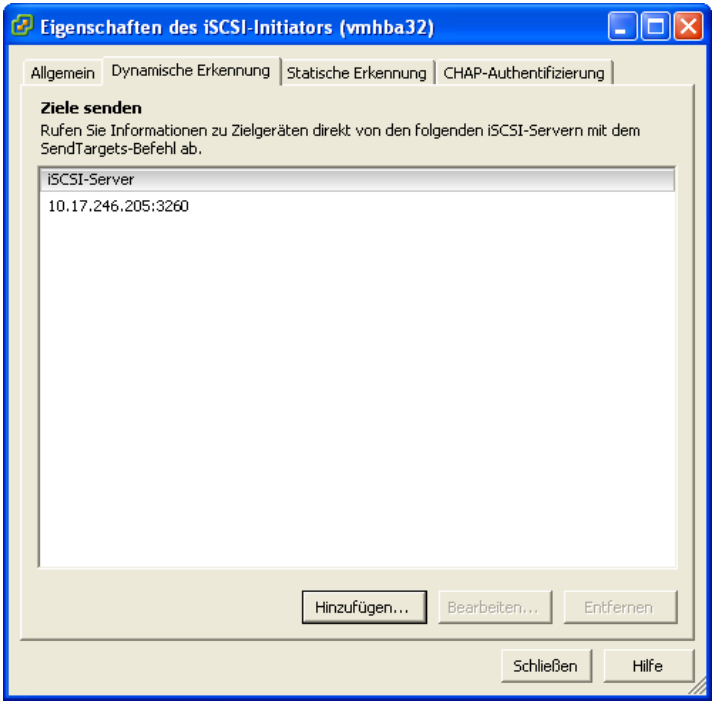
Sie müssen Zielerkennungsadressen einrichten, damit der Hardware-Initiator erkennen kann, welche Speicherressourcen im Netzwerk zur Verfügung stehen. Verwenden Sie dazu die dynamische oder statische Erkennung.

Siehe „Erkennungsmethoden“ auf Seite 118.

Bei der dynamischen Erkennung übergibt ein bestimmter iSCSI-Server eine Liste mit Zielen an Ihren ESX Server 3 zurück.

So richten Sie Zielerkennungsadressen mithilfe der dynamischen Erkennung ein

1 Klicken Sie im Dialogfeld **iSCSI-Initiator-Eigenschaften (iSCSI Initiator Properties)** auf die Registerkarte **Dynamische Erkennung (Dynamic Discovery)**.



2 Klicken Sie auf **Hinzufügen (Add)**, um einen neuen iSCSI-Server hinzuzufügen, den der ESX Server 3-Host für eine dynamische Erkennungssitzung verwenden kann.

3 Geben Sie in das Dialogfeld **Server als Sendeziele hinzufügen (Add Send Targets Server)** die IP-Adresse des iSCSI-Servers ein, und klicken Sie auf **OK**.

   Nachdem der ESX Server 3-Host die dynamische Erkennungssitzung mit diesem Server eingerichtet hat, antwortet der Server mit dem Bereitstellen einer Liste mit Zielen, die Ihrem ESX Server 3-Host zur Verfügung stehen. Die Namen und IP-Adressen dieser Ziele werden auf der Registerkarte **Statische Erkennung (Static Discovery)** angezeigt.

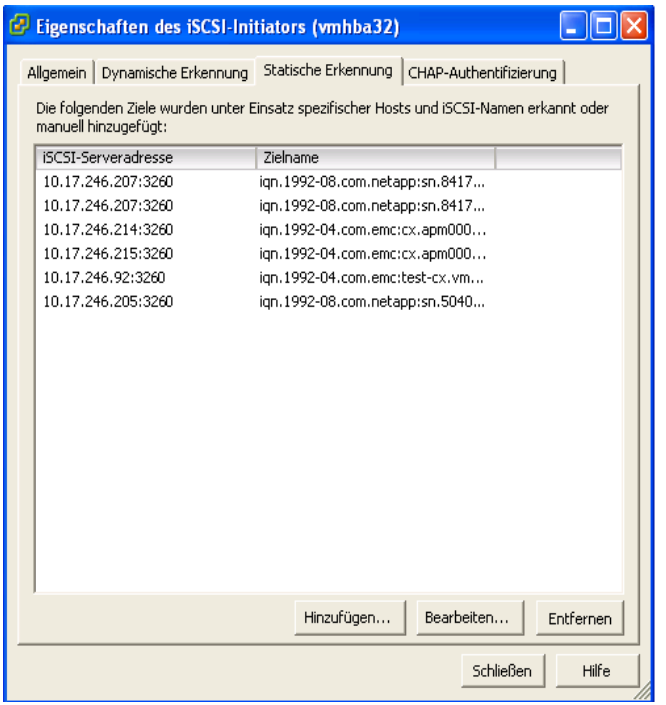
4 Um die IP-Adresse des iSCSI-Servers zu ändern oder den Server zu entfernen, wählen Sie die IP-Adresse aus und klicken auf **Bearbeiten (Edit)** oder **Entfernen (Remove)**.

Bei Hardware-Initiatoren können Sie neben der dynamischen Erkennungsmethode auch die statische Erkennung verwenden, bei der Sie die IP-Adressen und iSCSI-Namen der zu kontaktierenden Ziele manuell eingeben.

So richten Sie Zielerkennungsadressen mithilfe der statischen Erkennung ein

1 Klicken Sie im Dialogfeld **iSCSI-Initiator-Eigenschaften (iSCSI Initiator Properties)** auf die Registerkarte **Statische Erkennung (Static Discovery)**.

Wenn Sie zuvor die dynamische Erkennungsmethode verwendet haben, werden auf der Registerkarte alle Ziele angezeigt, die der iSCSI-Server dem ESX Server 3-Host bereitstellt.



2 Um ein Ziel hinzuzufügen, klicken Sie auf **Hinzufügen (Add)** und geben Sie die IP-Adresse und den vollständig qualifizierten Namen des Ziels ein.

3 Um ein bestimmtes Ziel zu ändern oder zu löschen, wählen Sie das Ziel aus, und klicken Sie auf **Bearbeiten (Edit)** oder **Entfernen (Remove)**.

HINWEIS Wenn Sie ein von der dynamischen Erkennung hinzugefügtes Ziel entfernen, kann das Ziel entweder bei einer erneuten Überprüfung, beim Zurücksetzen des HBA oder durch einen Neustart des Systems erneut zur Liste hinzugefügt werden.

Einrichten von CHAP-Parametern für Hardware-Initiatoren

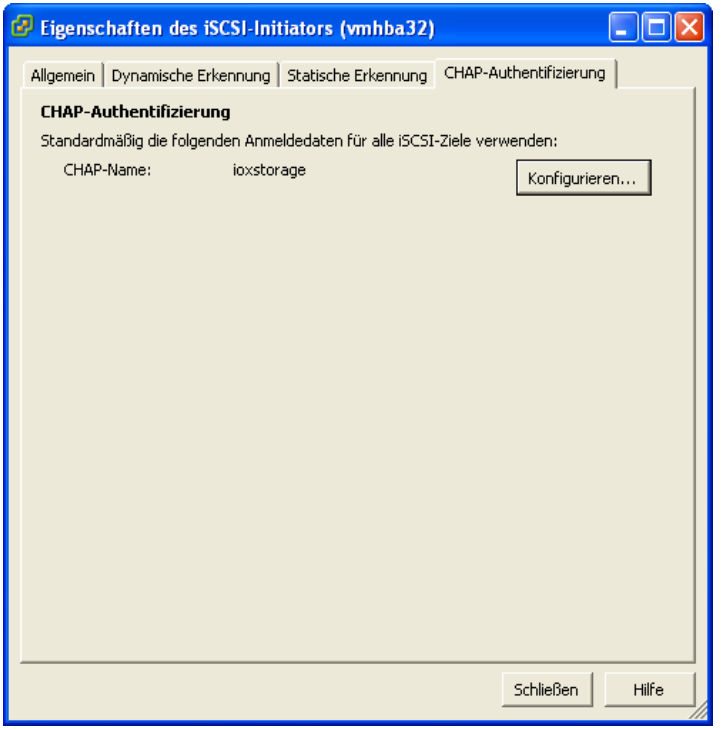
Prüfen Sie beim Konfigurieren Ihres Hardware-iSCSI-Initiators, ob CHAP für den iSCSI-Speicher aktiviert ist. Falls ja, aktivieren Sie das Protokoll für Ihren Initiator, und stellen Sie sicher, dass die CHAP-Authentifizierungsinformationen Ihrem iSCSI-Speicher entsprechen.

Siehe „iSCSI-Sicherheit“ auf Seite 118.

So richten Sie CHAP-Parameter für den Hardware-Initiator ein

1 Klicken Sie im Dialogfeld **iSCSI-Initiator-Eigenschaften (iSCSI Initiator Properties)** auf die Registerkarte **CHAP-Authentifizierung (CHAP Authentication)**.

Auf der Registerkarte werden die standardmäßigen CHAP-Parameter, falls vorhanden, angezeigt.



2 Um die vorhandenen CHAP-Parameter zu ändern, klicken Sie auf **Konfigurieren (Configure)**.

3 Damit CHAP auch weiterhin aktiviert bleibt, aktivieren Sie **Folgende CHAP-Anmeldeinformationen verwenden (Use the following CHAP credentials)**.

4 Geben Sie einen neuen CHAP-Namen ein, oder wählen Sie **Initiator-Namen verwenden (Use initiator name)**.

5 Geben Sie ggf. einen CHAP-Schlüssel an.

Alle neuen Ziele verwenden diesen CHAP-Schlüssel, um den Initiator zu authentifizieren.

6 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

HINWEIS Wenn Sie CHAP deaktivieren, bleiben bestehende Sitzungen aktiv, bis Sie den ESX Server 3-Host neu starten oder das Speichersystem eine Abmeldung erzwingt. Anschließend können Sie sich nicht mehr mit Zielen verbinden, die CHAP erfordern.

Hinzufügen von iSCSI-Speicher, auf den über Hardware-Initiatoren zugegriffen werden kann

Wenn Sie einen Datenspeicher auf einem SCSI-Speichergerät erstellen, auf das über einen Hardware-Initiator zugegriffen werden kann, führt Sie der Assistent zum Hinzufügen von Speicher durch die Konfiguration.

So erstellen Sie einen Datenspeicher auf einem Hardware-iSCSI-Gerät

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend unter **Hardware** auf **Speicher (Storage)**.

3 Klicken Sie auf **Speicher hinzufügen (Add Storage)**.

4 Markieren Sie den Speichertyp **Festplatte/LUN (Disk/LUN)**, und klicken Sie auf **Weiter (Next)**.

5 Wählen Sie das iSCSI-Gerät aus, das Sie für den Datenspeicher verwenden möchten, und klicken Sie auf **Weiter (Next)**.

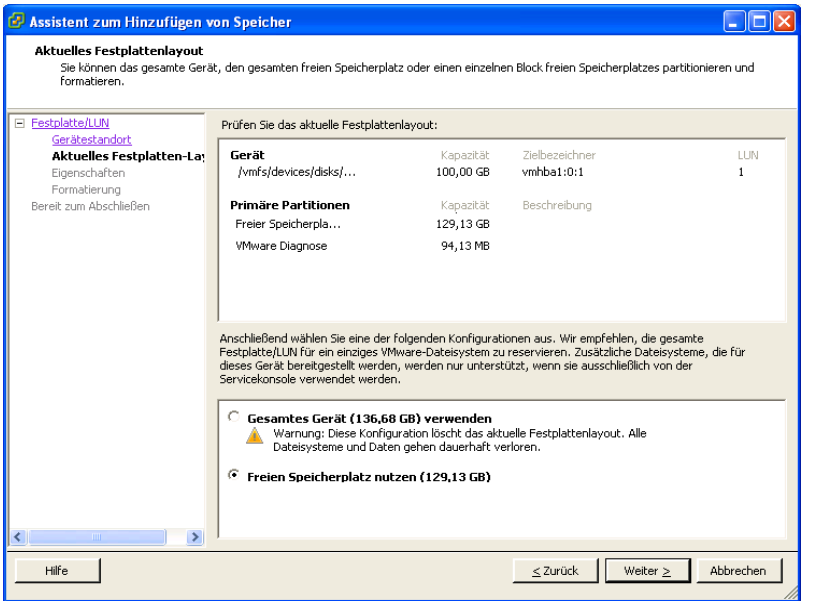
Die Seite **Aktuelles Festplattenlayout (Current Disk Layout)** wird angezeigt. Wenn die zu formatierende Festplatte leer ist, zeigt die Seite **Aktuelles Festplattenlayout (Current Disk Layout)** automatisch den gesamten Speicherplatz der Festplatte, der für die Konfiguration zur Verfügung steht.

6 Wenn die Festplatte nicht leer ist, überprüfen Sie im oberen Bereich auf der Seite **Aktuelles Festplattenlayout (Current Disk Layout)** das aktuelle Festplattenlayout, und wählen Sie im unteren Bereich eine Konfigurationsoption aus:

- **Gesamtes Gerät verwenden (Use the entire device)** – Wählen Sie diese Option, um die gesamte Festplatte oder LUN einem einzelnen VMFS-Datenspeicher zur Verfügung zu stellen. VMware empfiehlt das Aktivieren dieser Option.

WARNUNG Bei Wahl dieser Option werden zuvor auf diesem Gerät gespeicherte Dateisysteme und Daten dauerhaft gelöscht.

- **Freien Speicherplatz verwenden (Use free space)** – Wählen Sie diese Option, um einen VMFS-Datenspeicher im verbleibenden freien Speicherplatz auf der Festplatte bereitzustellen.


Assistent zum Hinzufügen von Speicher
Aktuelles Festplattenlayout
Sie können das gesamte Gerät, den gesamten freien Speicherplatz oder einen einzelnen Block freien Speicherplatzes partitionieren und formatieren.
Festplatte/LUN
Gerätestandort
Aktuelles Festplatten-Lay
Eigenschaften
Formatierung
Bereit zum Abschließen
Prüfen Sie das aktuelle Festplattenlayout:
Gerät
Kapazität
Zielbezeichner
LUN
/vmfs/devices/disks/...
100,00 GB
vmhba1:0:1
1
Primäre Partitionen
Kapazität
Beschreibung
Freier Speicherpla...
129,13 GB
VMware Diagnose
94,13 MB
Anschließend wählen Sie eine der folgenden Konfigurationen aus. Wir empfehlen, die gesamte Festplatte/LUN für ein einziges VMware-Dateisystem zu reservieren. Zusätzliche Dateisysteme, die für dieses Gerät bereitgestellt werden, werden nur unterstützt, wenn sie ausschließlich von der Servicekonsole verwendet werden.
Gesamtes Gerät (136,68 GB) verwenden
Warnung: Diese Konfiguration löscht das aktuelle Festplattenlayout. Alle Dateisysteme und Daten gehen dauerhaft verloren.
Freien Speicherplatz nutzen (129,13 GB)
Hilfe
< Zurück
Weiter >
Abbrechen

7 Klicken Sie auf **Weiter (Next)**.

8 Geben Sie auf der Seite **Festplatte/LUN–Eigenschaften (Disk/LUN–Properties)** einen Dateispeichernamen ein, und klicken Sie auf **Weiter (Next)**.

9 Ändern Sie bei Bedarf die Werte für das Dateisystem und die Größe des Datenspeichers. Standardmäßig wird der gesamte freie Speicherplatz des Speichergeräts zur Verfügung gestellt.

10 Klicken Sie auf **Weiter (Next)**.

11 Überprüfen Sie die Informationen zum Datenspeicher, und klicken Sie auf **Fertig (Finish)**.

Dadurch wird ein Datenspeicher auf dem hardware-initiierten iSCSI-Gerät erstellt.

12 Klicken Sie auf **Aktualisieren (Refresh)**.

Konfigurieren von Software-iSCSI-Initiatoren und Speicher

Bei der Verwendung von softwarebasiertem iSCSI können Sie einen normalen Netzwerkadapter verwenden, um das ESX Server 3-System an ein iSCSI-Remoteziel im IP-Netzwerk anzubinden. Der in den VMkernel integrierte Software-iSCSI-Initiator von ESX Server 3 ermöglicht diese Verbindung, indem er über den Protokollstapel mit dem Netzwerkadapter kommuniziert.

Bevor Sie Datenspeicher konfigurieren, die über Software-Initatoren auf den iSCSI-Speicher zugreifen, aktivieren Sie die Netzwerkkonnektivität, und konfigurieren Sie anschließend den iSCSI-Initator.

Einrichten des iSCSI-Speichers, auf den über Software-Initatoren zugegriffen werden kann

Führen Sie zur Vorbereitung und Einrichtung von Datenspeichern, die Software-Initatoren für den Zugriff auf das iSCSI-Speichergerät verwenden, die folgenden Schritte aus.

1 Erstellen Sie einen VMkernel-Port für die Verarbeitung des iSCSI-Netzwerkbetriebs.

Siehe „Netzwerkkonfiguration des VMkernels“ auf Seite 30 und „Netzwerkkonfiguration für Software-iSCSI-Speicher“ auf Seite 76.

2 Konfigurieren Sie eine Servicekonsolenverbindung für softwarebasiertes iSCSI.

Siehe „Öffnen von Firewallports für unterstützte Dienste und Verwaltungs-Agenten“ auf Seite 198.

3 Konfigurieren Sie den Software-iSCSI-Initiator.

Siehe „Konfigurieren eines Software-iSCSI-Initiators“ auf Seite 129.

4 Suchen Sie erneut nach neuen iSCSI-LUNs.

Siehe „Starten einer erneuten Prüfung“ auf Seite 134.

5 Richten Sie den Datenspeicher ein.

Siehe „Hinzufügen von iSCSI-Speicher, auf den über Software-Initiatoren zugegriffen werden kann“ auf Seite 131.

Anzeigen der Eigenschaften von Software-iSCSI-Initiatoren

Der Software-iSCSI-Adapter, den das ESX Server 3-System verwendet, um auf iSCSI-Speichergeräte zuzugreifen, wird in der Liste der verfügbaren Adapter angezeigt. Dessen Eigenschaften können Sie mit dem VI-Client anzeigen.

So zeigen Sie die Eigenschaften des Software-iSCSI-Initiators an

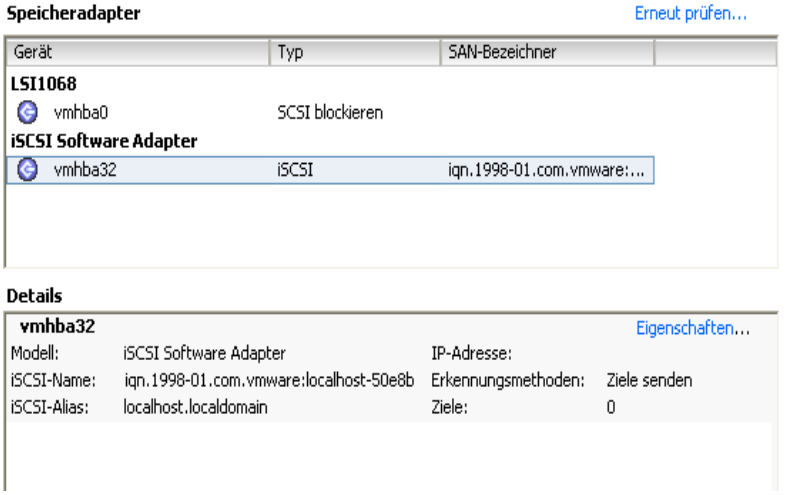
1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend unter **Hardware** auf **Speicheradapter (Storage Adapters)**.

Ein Verzeichnis der verfügbaren Speicheradapter wird angezeigt.

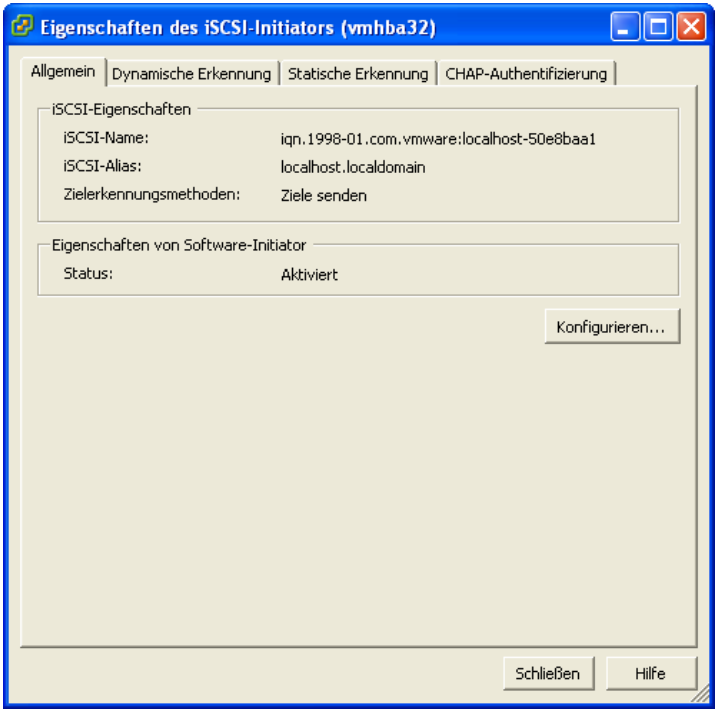
3 Wählen Sie unter **iSCSI-Software-Adapter (iSCSI Software Adapter)** den verfügbaren Software-Initiator aus.

Wird der Initiator aktiviert, werden dazugehörige Details angezeigt, u. a. Modell, IP-Adresse, iSCSI-Name, Erkennungsmethoden, iSCSI-Alias und erkannte Ziele.



4 Klicken Sie auf **Eigenschaften (Properties)**.

Das Dialogfeld **iSCSI-Initiator-Eigenschaften (iSCSI Initiator Properties)** wird angezeigt. Auf der Registerkarte **Allgemein (General)** werden zusätzliche Merkmale des Software-Initiators angezeigt.



Sie können den Software-Initiator jetzt konfigurieren oder seine Standardmerkmale ändern.

Konfigurieren eines Software-iSCSI-Initiators

Bei der Konfiguration des Software-iSCSI-Initiators aktivieren Sie den Initiator und richten dessen Zieladressen ein. Darüber hinaus empfiehlt VMware die Einrichtung von CHAP-Parametern. Nach der Konfiguration des Software-iSCSI-Initiators müssen Sie erneut nach Speichergeräten suchen, damit alle LUNs, auf die der Initiator zugreifen kann, im Verzeichnis der für das ESX Server 3-System verfügbaren Speichergeräte aufgelistet werden. Siehe „Starten einer erneuten Prüfung“ auf Seite 134.

Aktivieren von Software-iSCSI-Initiatoren

Aktivieren Sie Ihren Software-iSCSI-Initiator, damit er von ESX Server 3 verwendet werden kann.

So aktivieren Sie den Software-iSCSI-Initiator

1 Klicken Sie im Dialogfeld **Eigenschaften des iSCSI-Initiators (iSCSI Initiator Properties)** auf die Schaltfläche **Konfigurieren (Configure)**.

2 Aktivieren Sie das Kontrollkästchen **Aktiviert (Enabled)**, um den Initiator zu aktivieren.

3 Um den Standard-iSCSI-Namen für den Initiator zu ändern, geben Sie einen neuen Namen ein.

Stellen Sie sicher, dass der eingegebene Name ordnungsgemäß formatiert ist. Andernfalls können einige Speichergeräte den Software-iSCSI-Initiator ggf. nicht erkennen. Siehe „Benennungskonventionen“ auf Seite 117.

4 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

Einrichten von Erkennungsadressen für Software-Initiatoren

Sie müssen Zielerkennungsadressen einrichten, damit der Softwareware-Initiator erkennen kann, welche Speicherressourcen im Netzwerk zur Verfügung stehen.

HINWEIS Für Software-Initatoren steht nur die dynamische Erkennungsmethode zur Verfügung.

Siehe „Erkennungsmethoden“ auf Seite 118.

So richten Sie Zielerkennungsadressen für den Software-Initiator ein

1 Klicken Sie im Dialogfeld **iSCSI-Initiator-Eigenschaften (iSCSI Initiator Properties)** auf die Registerkarte **Dynamische Erkennung (Dynamic Discovery)**.

2 Klicken Sie auf **Hinzufügen (Add)**, um ein neues iSCSI-Ziel hinzuzufügen, das der ESX Server 3-Host für eine dynamische Erkennungssitzung verwenden kann.

3 Geben Sie die Server-IP-Adresse für **Ziele senden (Send Targets)** ein und klicken Sie auf **OK**.

4 Wenn Sie einen bestimmten „Ziele senden“-Server ändern oder löschen möchten, markieren Sie den Server und klicken Sie auf **Bearbeiten (Edit)** oder **Entfernen (Remove)**.

Einrichten von CHAP-Parametern für Software-Initiatoren

Prüfen Sie beim Konfigurieren Ihres Software-iSCSI-Initiators, ob CHAP für den iSCSI-Speicher aktiviert ist. Falls ja, aktivieren Sie das Protokoll für den Initiator, und stellen Sie sicher, dass die CHAP-Authentifizierungsinformationen Ihrem iSCSI-Speicher entsprechen.

Siehe „iSCSI-Sicherheit“ auf Seite 118.

So richten Sie CHAP-Parameter für den Software-Initiator ein

1 Klicken Sie im Dialogfeld **iSCSI-Initiator-Eigenschaften (iSCSI Initiator Properties)** auf die Registerkarte **CHAP-Authentifizierung (CHAP Authentication)**.

2 Klicken Sie zum Angeben von CHAP-Parametern auf **Konfigurieren (Configure)**.

3 Damit CHAP auch aktiviert bleibt, aktivieren Sie **Folgende CHAP-Anmeldeinformationen verwenden (Use the following CHAP credentials)**.

4 Geben Sie einen CHAP-Namen ein, oder wählen Sie **Initiator-Namen verwenden (Use initiator name)**.

5 Geben Sie ggf. einen CHAP-Schlüssel an.

   Alle neuen Ziele verwenden diesen CHAP-Schlüssel, um den Initiator zu authentifizieren.

6 Klicken Sie auf **OK**, um Ihre Änderungen zu speichern.

HINWEIS Wenn Sie CHAP deaktivieren, bleiben bestehende Sitzungen aktiv, bis Sie den ESX Server 3-Host neu starten oder das Speichersystem eine Abmeldung erzwingt. Anschließend können Sie sich nicht mehr mit Zielen verbinden, die CHAP erfordern.

Hinzufügen von iSCSI-Speicher, auf den über Software-Initiatoren zugegriffen werden kann

Wenn Sie einen Datenspeicher auf einem SCSI-Speichergerät erstellen, auf das über einen Software-Initiator zugegriffen werden kann, führt Sie der Assistent zum Hinzufügen von Speicher durch die Konfiguration.

So erstellen Sie einen Datenspeicher auf einem iSCSI-Gerät, auf das über Software-Initiatoren zugegriffen wird

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend unter **Hardware** auf **Speicher (Storage)**.

3 Klicken Sie auf **Speicher hinzufügen (Add Storage)**.

4 Markieren Sie den Speichertyp **Festplatte/LUN (Disk/LUN)**, und klicken Sie auf **Weiter (Next)**.

5 Wählen Sie das iSCSI-Gerät aus, das Sie für den Datenspeicher verwenden möchten, und klicken Sie auf **Weiter (Next)**.

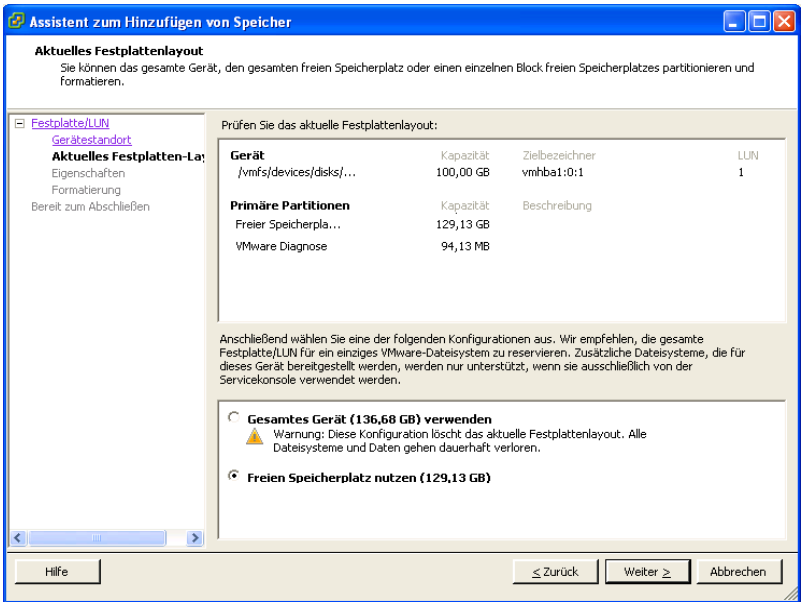
   Die Seite **Aktuelles Festplattenlayout (Current Disk Layout)** wird angezeigt. Wenn die zu formatierende Festplatte leer ist, zeigt die Seite **Aktuelles Festplattenlayout (Current Disk Layout)** automatisch den gesamten Speicherplatz der Festplatte, der für die Konfiguration zur Verfügung steht.

6 Wenn die Festplatte nicht leer ist, überprüfen Sie im oberen Bereich auf der Seite **Aktuelles Festplattenlayout (Current Disk Layout)** das aktuelle Festplattenlayout, und wählen Sie im unteren Bereich eine Konfigurationsoption aus:

   - **Gesamtes Gerät verwenden (Use the entire device)** – Wählen Sie diese Option, um die gesamte Festplatte oder LUN einem einzelnen VMFS-Datenspeicher zur Verfügung zu stellen. VMware empfiehlt das Aktivieren dieser Option.

WARNUNG Bei Wahl dieser Option werden zuvor auf diesem Gerät gespeicherte Dateisysteme und Daten dauerhaft gelöscht.

- **Freien Speicherplatz verwenden (Use free space)** – Wählen Sie diese Option, um einen VMFS-Datenspeicher im verbleibenden freien Speicherplatz auf der Festplatte bereitzustellen.


Assistent zum Hinzufügen von Speicher
Aktuelles Festplattenlayout
Sie können das gesamte Gerät, den gesamten freien Speicherplatz oder einen einzelnen Block freien Speicherplatzes partitionieren und formatieren.
Festplatte/LUN
Gerätestandort
Aktuelles Festplatten-Lay
Eigenschaften
Formatierung
Bereit zum Abschließen
Prüfen Sie das aktuelle Festplattenlayout:
Gerät
Kapazität
Zielbezeichner
LUN
/vmfs/devices/disks/...
100,00 GB
vmhba1:0:1
1
Primäre Partitionen
Kapazität
Beschreibung
Freier Speicherpla...
129,13 GB
VMware Diagnose
94,13 MB
Anschließend wählen Sie eine der folgenden Konfigurationen aus. Wir empfehlen, die gesamte Festplatte/LUN für ein einziges VMware-Dateisystem zu reservieren. Zusätzliche Dateisysteme, die für dieses Gerät bereitgestellt werden, werden nur unterstützt, wenn sie ausschließlich von der Servicekonsole verwendet werden.
Gesamtes Gerät (136,68 GB) verwenden
Warnung: Diese Konfiguration löscht das aktuelle Festplattenlayout. Alle Dateisysteme und Daten gehen dauerhaft verloren.
Freien Speicherplatz nutzen (129,13 GB)
Hilfe
< Zurück
Weiter >
Abbrechen

7 Klicken Sie auf **Weiter (Next)**.

8 Geben Sie auf der Seite **Festplatte/LUN–Eigenschaften (Disk/LUN–Properties)** einen Dateispeichernamen ein, und klicken Sie auf **Weiter (Next)**.

9 Ändern Sie bei Bedarf die Werte für das Dateisystem und die Größe des Datenspeichers. Standardmäßig wird der gesamte freie Speicherplatz des Speichergeräts zur Verfügung gestellt.

10 Klicken Sie auf **Weiter (Next)**.

11 Überprüfen Sie die Informationen zum Datenspeicher, und klicken Sie auf **Fertig (Finish)**.

Dadurch wird ein Datenspeicher auf einem Software-iSCSI-Speichergerät erstellt.

12 Klicken Sie auf **Aktualisieren (Refresh)**.

Starten einer erneuten Prüfung

Führen Sie nach folgenden Ereignissen eine erneute Prüfung durch:

- Wenn Änderungen an den Speicherfestplatten oder den für das ESX Server 3-System verfügbaren LUNs vorgenommen wurden.
- Wenn Änderungen an Speicheradaptern vorgenommen werden.
- Wenn Sie einen neuen Datenspeicher hinzufügen oder einen vorhandenen entfernen.
- Wenn Sie einen vorhandenen Datenspeicher neu konfigurieren, z. B. wenn Sie eine neue Erweiterung hinzufügen.

HINWEIS Nachdem Sie alle Pfade zu einer LUN maskiert haben, prüfen Sie erneut alle Adapter mit Pfaden zur LUN, um die Konfiguration zu aktualisieren.

So führen Sie eine erneute Prüfung aus

1. Wählen Sie im VI-Client einen Host aus, und klicken Sie auf die Registerkarte **Konfiguration (Configuration)**.
2. Wählen Sie unter **Hardware** die Option **Speicheradapter (Storage Adapters)**, und klicken Sie über dem Bereich **Speicheradapter (Storage Adapters)** auf **Erneut prüfen (Rescan)**.

   HINWEIS Sie können auch mit der rechten Maustaste auf einzelne Adapter klicken und auf **Erneut prüfen (Rescan)** klicken, wenn Sie nur diesen Adapter erneut prüfen möchten.

   ---

3. Wenn neue Festplatten oder LUNs erkannt werden sollen, aktivieren Sie **Auf neue Speichergeräte prüfen (Scan for New Storage Devices)**.

   Wenn neue LUNs erkannt werden, werden diese in der Liste **Festplatten/LUN (disk/LUN)** angezeigt.
4. Um neue Datenspeicher zu erkennen oder einen Dateispeicher nach einer Konfigurationsänderung zu aktualisieren, wählen Sie **Auf neue VMFS-Volumes prüfen (Scan for New VMFS Volumes)** aus.

   Wenn neue Datenspeicher oder VMFS-Volumes erkannt werden, werden diese in der Datenspeicherliste angezeigt.

Network Attached Storage (NAS)

In diesem Abschnitt wird Network Attached Storage (NAS) behandelt.

ESX Server 3 unterstützt NAS über das NFS-Protokoll.

Verwendung von NFS durch virtuelle Maschinen

Das von ESX Server 3 unterstützte NFS-Protokoll ermöglicht die Kommunikation zwischen einem NFS-Client und einem NFS-Server. Der Client sendet Informationsanfragen an den Server, der das Ergebnis zurückgibt.

Über den in ESX Server 3 integrierten NFS-Client können Sie auf den NFS-Server zugreifen und NFS-Volumes zum Speichern verwenden. ESX Server 3 unterstützt ausschließlich NFS Version 3 über TCP/IP.

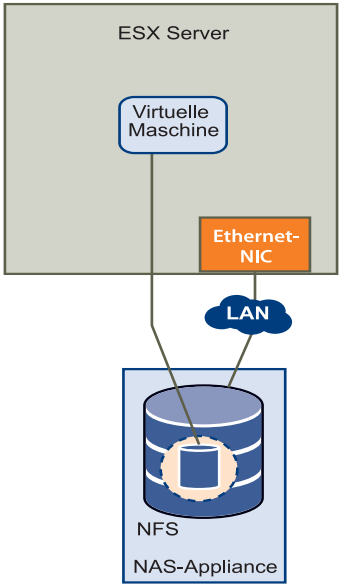
Mit dem VI-Client können Sie NFS-Volumes als Datenspeicher konfigurieren. Konfigurierte NFS-Datenspeicher werden im VI-Client angezeigt und können genau wie VMFS-basierte Datenspeicher zur Speicherung virtueller Festplattendateien verwendet werden.

Die von Ihnen in NFS-basierten Datenspeichern erstellten virtuellen Festplatten verwenden ein Festplattenformat, das vom NFS-Server vorgegeben wird. In der Regel ist dies ein Thin-Festplattenformat, das eine bedarfsgerechte Speicherplatzzuordnung erfordert. Wenn der Speicherplatz auf der virtuellen Maschine während des Schreibvorgangs auf die Festplatte nicht mehr ausreicht, erhalten Sie vom VI-Client eine Benachrichtigung darüber, dass zusätzlicher Speicherplatz erforderlich ist. Sie können dann aus den folgenden Optionen wählen:

- Zusätzlichen Speicherplatz auf dem Volume freimachen, damit der Schreibvorgang auf die Festplatte fortgesetzt werden kann.
- Beenden der virtuellen Maschinensitzung. Durch Beenden der Sitzung wird die virtuelle Maschine heruntergefahren.

Abbildung 6-4 zeigt eine virtuelle Maschine, die ein NFS-Volume zur Speicherung ihrer Dateien verwendet.

Abbildung 6-4. NFS-Speicher



In dieser Konfiguration stellt ESX Server 3 eine Verbindung zum NFS-Server her, auf dem die virtuellen Festplattendateien gespeichert sind.

WARNUNG Wenn ESX Server 3 auf eine virtuelle Festplattendatei auf einem NFS-basierten Datenspeicher zugreift, wird im gleichen Verzeichnis, in dem sich die Festplattendatei befindet, eine spezielle `.lck–XXX`-Sperrdatei erstellt, um zu verhindern, dass andere ESX Server 3-Hosts auf diese virtuelle Festplattendatei zugreifen. Diese `.lck–XXX`-Sperrdatei darf nicht gelöscht werden, da sonst die aktive virtuelle Maschine nicht auf ihre virtuelle Festplattendatei zugreifen kann.

NFS-Volumes und delegierte Benutzer für virtuelle Maschine

Wenn Sie virtuelle Maschinen in einem NFS-basierten Datenspeicher erstellen, konfigurieren oder verwalten möchten, müssen Sie einem bestimmten Benutzer, dem delegierten Benutzer, NFS-Zugriffsrechte zuweisen.

Der delegierte Benutzer für den ESX Server 3-Host ist standardmäßig `root`. Nicht alle NFS-Volumes akzeptieren jedoch `Root` als delegierten Benutzer. In einigen Fällen ist es möglicherweise angebracht, dass der NFS-Administrator die Volumes mit aktivierter Option `root squash` exportiert, um die NFS-Volumes vor unbefugtem Zugriff zu schützen. Wenn die Option `root squash` aktiviert ist, behandelt der NFS-Server den Root-Zugriff wie einen unberechtigten Benutzerzugriff und verweigert möglicherweise den Zugriff des ESX Server 3-Hosts auf Dateien der virtuellen Maschine, die auf dem NFS-Volume gespeichert sind.

Sie können dem delegierten Benutzer mithilfe der experimentellen ESX Server 3-Funktionen eine andere Identität zuweisen. Diese Identität muss mit der Identität des Besitzers des Verzeichnisses auf dem NFS-Server übereinstimmen. Ansonsten kann der ESX Server 3-Host keine Vorgänge auf Dateiebene durchführen.

Siehe „Delegierte VM-Benutzer für NFS-Speicher“ auf Seite 242.

VORSICHT Das Ändern des delegierten Benutzers für einen ESX Server 3-Host ist experimentell. Darüber hinaus bietet VMware derzeit nur eingeschränkten Support für diese Funktion.

Konfigurieren von ESX Server 3 für den Zugriff auf NFS-Volumes

Damit NFS auf Daten auf Remoteservern zugreifen kann, muss es an das Netzwerk angebunden sein. Vor der Konfiguration von NFS muss daher zuerst die Netzwerkverbindung für VMotion und den IP-Speicher konfiguriert werden.

Weitere Informationen zur Netzwerkkonfiguration finden Sie unter „Netzwerkkonfiguration des VMkernels“ auf Seite 30.

Erstellen eines NFS-basierten Datenspeichers

Wenn Sie einen Datenspeicher auf einem NFS-Volume erstellen, führt Sie der Assistent zum Hinzufügen von Speicher durch die Konfiguration.

So mounten Sie ein NFS-Volume

1. Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.
2. Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend unter **Hardware** auf **Speicher (Storage)**.
3. Klicken Sie auf **Speicher hinzufügen (Add Storage)**.

4 Wählen Sie **Netzwerkdateisystem (Network File System)** als Speichertyp aus, und klicken Sie auf **Weiter (Next)**.

5 Geben Sie den Server-, den Mount-Punkt-Ordner- und den Datenspeichernamen ein.

6 Klicken Sie auf **Weiter (Next)**.

7 Überprüfen Sie auf der Übersichtsseite für das Netzwerkdateisystem (NFS) die Konfigurationsoptionen, und klicken Sie auf **Fertig (Finish)**.

Erstellen einer Diagnosepartition

Zum Ausführen des ESX Server 3-Hosts wird eine Diagnosepartition bzw. Dump-Partition benötigt, um Core-Dumps für das Debuggen und den technischen Support zu speichern. Die Diagnosepartition kann auf einer lokalen Festplatte oder einer privaten oder freigegebenen SAN-LUN erstellt werden.

Es ist jedoch nicht möglich, eine Diagnosepartition auf einer iSCSI-LUN zu speichern, auf die über einen Software-Initiator zugegriffen wird.

Für jeden ESX Server 3-Host ist eine Diagnosepartition mit 100 MB erforderlich. Wenn mehrere ESX Server 3-Hosts ein gemeinsames SAN verwenden, konfigurieren Sie pro Host eine Diagnosepartition mit 100 MB.

HINWEIS Wenn Sie während der ESX Server 3-Installation **Empfohlene Partitionierung (Recommended Partitioning)** gewählt haben, wurde vom Installationsprogramm bereits automatisch eine Diagnosepartition erstellt. Die Option **Diagnose (Diagnostic)** wird nicht auf der Seite **Speichertyp auswählen (Select Storage Type)** angezeigt. Wenn Sie während der Installation **Erweiterte Partitionierung (Advanced Partitioning)** gewählt und keine Diagnosepartition angegeben haben, müssen Sie nun eine konfigurieren. Weitere Informationen zur Installation von ESX Server 3 finden Sie im *Installationshandbuch (Installation Guide)*.

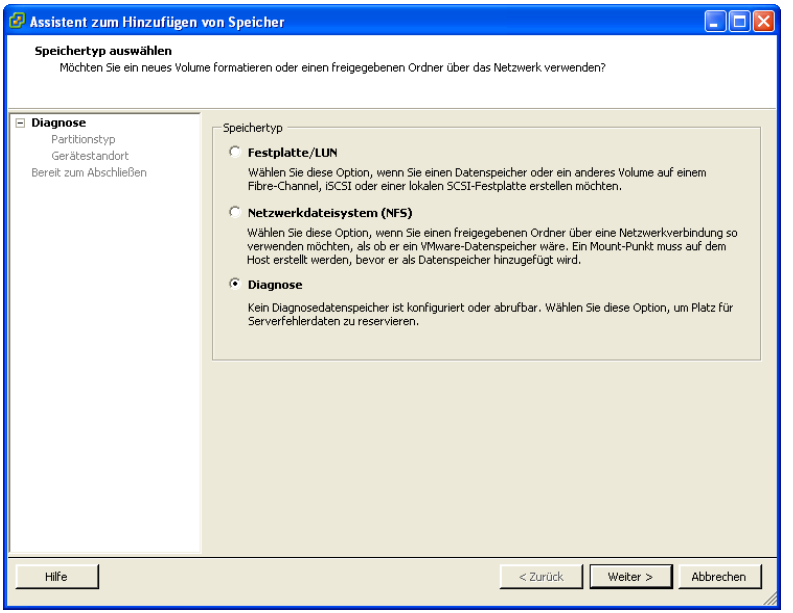
So erstellen Sie eine Diagnosepartition

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend unter **Hardware** auf **Speicher (Storage)**.

3 Klicken Sie auf **Speicher hinzufügen (Add Storage)**.

Das Dialogfeld **Speichertyp auswählen (Select Storage Type)** wird angezeigt.


Assistent zum Hinzufügen von Speicher
Speichertyp auswählen
Möchten Sie ein neues Volume formatieren oder einen freigegebenen Ordner über das Netzwerk verwenden?
Diagnose
Partitionstyp
Gerätestandort
Bereit zum Abschließen
Speichertyp
Festplatte/LUN
Wählen Sie diese Option, wenn Sie einen Datenspeicher oder ein anderes Volume auf einem Fibre-Channel, iSCSI oder einer lokalen SCSI-Festplatte erstellen möchten.
Netzwerkdateisystem (NFS)
Wählen Sie diese Option, wenn Sie einen freigegebenen Ordner über eine Netzwerkverbindung so verwenden möchten, als ob er ein VMware-Datenspeicher wäre. Ein Mount-Punkt muss auf dem Host erstellt werden, bevor er als Datenspeicher hinzugefügt wird.
Diagnose
Kein Diagnosedatenspeicher ist konfiguriert oder abrufbar. Wählen Sie diese Option, um Platz für Serverfehlerdaten zu reservieren.
Hilfe
< Zurück
Weiter >
Abbrechen

4 Wählen Sie **Diagnose (Diagnostic)** aus, und klicken Sie auf **Weiter (Next)**.

Wenn **Diagnose (Diagnostic)** nicht als Option angezeigt wird, ist auf dem ESX Server-Host bereits eine Diagnosepartition vorhanden. Sie können die Diagnosepartition auf dem Host abfragen und durchsuchen, indem Sie den Befehl `esxcfg-dumppart` in die Servicekonsole eingeben. Siehe „Befehle für den technischen Support von ESX Server 3“ auf Seite 291.

5 Legen Sie die Art der Diagnosepartition fest:

- **Privater lokaler Speicher (Private Local)** – Erstellt die Diagnosepartition auf einer lokalen Festplatte. In dieser Partition werden ausschließlich Fehlerinformationen für den ESX Server 3-Host gespeichert.
- **Privater SAN-Speicher (Private SAN Storage)** – Erstellt die Diagnosepartition auf einer nicht freigegebenen SAN-LUN. In dieser Partition werden ausschließlich Fehlerinformationen für den ESX Server 3-Host gespeichert.
- **Freigegebener SAN-Speicher (Shared SAN Storage)** – Erstellt die Diagnosepartition auf einer freigegebenen SAN-LUN. In dieser Partition, auf die mehrere Hosts zugreifen, können ggf. Fehlerinformationen für mehrere Host gespeichert werden.

Klicken Sie auf **Weiter (Next)**.

6 Wählen Sie das Gerät, das Sie für die Diagnosepartition verwenden möchten, und klicken Sie auf **Weiter (Next)**.

7 Überprüfen Sie die Konfigurationsinformationen für die Partition, und klicken Sie auf **Fertig (Finish)**.

7 Speicherverwaltung

Dieses Kapitel enthält Informationen zur Verwaltung bestehender Datenspeicher und Dateisysteme, die Datenspeicher enthalten. In diesem Kapitel werden folgende Themen behandelt:

- „Verwalten von Datenspeichern“ auf Seite 142
- „Bearbeiten von VMFS-Datenspeichern“ auf Seite 143
- „Verwalten mehrerer Pfade“ auf Seite 146
- „Die vmkfstools-Befehle“ auf Seite 154

Verwalten von Datenspeichern

Das ESX Server 3-System nutzt Datenspeicher, um alle Dateien, die seinen virtuellen Maschinen zugeordnet sind, zu speichern. Der Datenspeicher ist eine logische Speichereinheit, die Festplattenspeicher auf einem physischen Gerät, auf einer Festplattenpartition oder übergreifend auf mehreren physischen Geräten verwendet. Der Datenspeicher kann sich auf verschiedenen Typen physischer Geräte wie SCSI, iSCSI, Fibre-Channel-SANs oder NFS befinden.

HINWEIS Als Alternative zur Verwendung des Datenspeichers kann Ihre virtuelle Maschine über eine Zuordnungsdatei (RDM) direkt auf Raw-Geräte zugreifen. Siehe „Raw-Gerätezuordnungseigenschaften“ auf Seite 161.

Weitere Informationen zu Datenspeichern finden Sie unter „Datenspeicher“ auf Seite 95.

Es gibt zwei Möglichkeiten, dem VI-Client Datenspeicher hinzufügen:

- Erkennung, sobald ein Host der Bestandsliste hinzugefügt wird. Wenn Sie der Bestandsliste einen Host hinzufügen, zeigt der VI-Client alle Datenspeicher an, die der Host erkennen kann.
- Erstellung auf einem verfügbaren Speichergerät. Über den Befehl **Speicher hinzufügen (Add Storage)** können Sie einen neuen Datenspeicher erstellen und konfigurieren.

Nachdem Sie die Datenspeicher erstellt haben, können Sie die Dateien virtueller Maschinen darin speichern. Gegebenenfalls können Sie die Datenspeicher auch ändern. So können Sie zum Beispiel Erweiterungen für den Datenspeicher hinzufügen oder Datenspeicher umbenennen oder löschen.

Nicht mehr verwendete Datenspeicher können entfernt werden.

VORSICHT Durch das Entfernen eines Datenspeichers vom ESX Server 3-System wird die Verbindung zwischen dem System und dem Speichergerät mit dem Datenspeicher unterbrochen, und alle Funktionen dieses Speichergeräts werden beendet.

Sie können Datenspeicher nicht entfernen, wenn sich darin virtuelle Festplatten einer aktuell ausgeführten virtuellen Maschine befinden.

So entfernen Sie einen Datenspeicher

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Speicher (Storage)**.

3 Wählen Sie den zu löschenden Datenspeicher aus, und klicken Sie auf **Entfernen (Remove)**.

4 Bestätigen Sie, dass Sie den Datenspeicher entfernen möchten.

5 Führen Sie auf allen Servern, auf denen der Datenspeicher angezeigt wird, eine erneute Prüfung durch.

Bearbeiten von VMFS-Datenspeichern

Datenspeicher im VMFS-Format werden auf SCSI-basierten Speichergeräten bereitgestellt.

Nach der Erstellung eines VMFS-basierten Datenspeichers können Sie diesen umbenennen oder erweitern. VMFS-2-Datenspeicher können in das VMFS-3-Format aktualisiert werden.

Aktualisieren von Datenspeichern

ESX Server 3 umfasst VMFS Version 3 (VMFS-3). Wenn der Datenspeicher mit VMFS-2 formatiert wurde, können Sie die auf VMFS-2 gespeicherten Dateien zwar lesen, aber nicht verwenden. Um die Dateien verwenden zu können, müssen Sie VMFS-2 auf VMFS-3 aktualisieren.

Wenn Sie ein Upgrade von VMFS-2 auf VMFS-3 durchführen, stellt der Mechanismus zur Dateisperrung von ESX Server 3 sicher, dass während der Konvertierung keine Remote-ESX Server 3- bzw. keine lokalen Prozesse auf das VMFS-Volume zugreifen. ESX Server 3 behält alle Dateien im Datenspeicher bei.

Vor der Aktualisierung werden als Vorsichtsmaßnahme folgende Schritte empfohlen:

- Akzeptieren oder verwerfen Sie alle Änderungen an virtuellen Festplatten auf dem VMFS 2-Volume, für das ein Upgrade durchgeführt werden soll.
- Sichern Sie das zu aktualisierende VMFS-2-Volume.
- Stellen Sie sicher, dass das VMFS-2-Volume nicht von aktiven virtuellen Maschinen verwendet wird.
- Stellen Sie sicher, dass kein anderer ESX Server-Host auf das VMFS-2-Volume zugreift.

VORSICHT Die Konvertierungsvorgang von VMFS-2 in VMFS-3 ist nicht umkehrbar. Nach der Konvertierung des VMFS-basierten Datenspeichers in VMFS-3 ist eine Rückkonvertierung in VMFS-2 nicht mehr möglich.

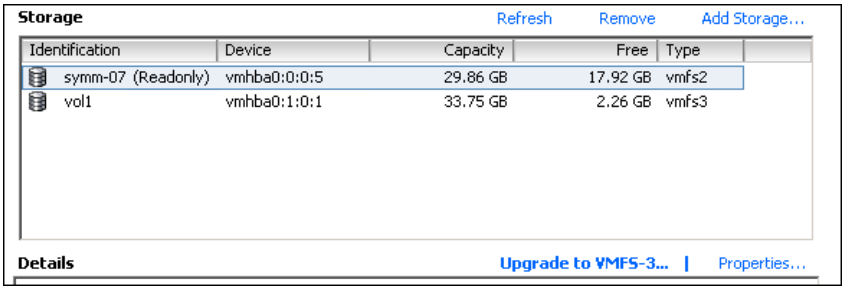
Damit das Upgrade des Dateisystems VMFS-2 möglich ist, sollte die Dateiblockgröße nicht über 8 MB hinausgehen.

So aktualisieren Sie VMFS-2 in VMFS-3

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Speicher (Storage)**.

3 Wählen Sie den Datenspeicher, der das VMFS-2-Format verwendet.



4 Klicken Sie auf **Auf VMFS-3 aktualisieren (Upgrade to VMFS-3)**.

5 Führen Sie auf allen Hosts, auf denen der Datenspeicher angezeigt wird, eine erneute Prüfung durch.

Ändern des Namens von Datenspeichern

Der Name eines vorhandenen VMFS-basierten Datenspeichers kann geändert werden.

So ändern Sie den Namen des Datenspeichers

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Speicher (Storage)**.

3 Markieren Sie den Datenspeicher, den Sie umbenennen möchten, und klicken Sie auf **Eigenschaften (Properties)**.

4 Klicken Sie unter **Allgemein (General)** auf **Ändern (Change)**.

5 Geben Sie den neuen Datenspeichernamen ein, und klicken Sie auf **OK**.

Hinzufügen von Erweiterungen zu Datenspeichern

Sie können einen Datenspeicher im VMFS-Format erweitern, indem Sie eine Festplattenpartition als Erweiterung einbinden. Der Datenspeicher kann sich über 32 physische Speichererweiterungen erstrecken.

Sie können die neuen Erweiterungen für den Datenspeicher dynamisch erstellen, wenn es erforderlich ist, neue virtuelle Maschinen in diesem Datenspeicher zu erstellen oder wenn die virtuellen Maschinen, die in diesem Datenspeicher ausgeführt werden, zusätzlichen Speicherplatz erfordern.

So fügen Sie Erweiterungen einem Datenspeicher hinzu

1. Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.
2. Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Speicher (Storage)**.
3. Wählen Sie den zu erweiternden Datenspeicher aus, und klicken Sie auf **Eigenschaften (Properties)**.
4. Klicken Sie unter **Erweiterungen (Extents)** auf **Erweiterung hinzufügen (Add Extent)**.
5. Wählen Sie die Festplatte aus, die Sie als neue Erweiterung hinzufügen möchten, und klicken Sie auf **Weiter (Next)**.
6. Überprüfen Sie das aktuelle Layout der Festplatte, die Sie für die Erweiterung verwenden möchten, um sicherzustellen, dass auf der Festplatte keine wichtigen Daten gespeichert sind.

VORSICHT Wenn die hinzuzufügende Festplatte oder Partition zuvor formatiert wurde, wird sie erneut formatiert, und sämtliche Dateisysteme und Daten, die sich auf der Festplatte oder Partition befinden, werden gelöscht.

7. Geben Sie die Kapazität der Erweiterung an.

   Standardmäßig wird der gesamte freie Speicherplatz des Speichergeräts zur Verfügung gestellt.
8. Klicken Sie auf **Weiter (Next)**.
9. Überprüfen Sie das vorgeschlagene Layout der Erweiterung und die neue Konfiguration des Datenspeichers, und klicken Sie anschließend auf **Fertig (Finish)**.
10. Führen Sie auf allen Servern, auf denen der Datenspeicher angezeigt wird, eine erneute Prüfung durch.

Verwalten mehrerer Pfade

Damit die Verbindung zwischen dem ESX Server 3-Host und dem DAS- bzw. NAS-Speicher nicht unterbrochen wird, unterstützt ESX Server 3 das so genannte Multipathing. *Multipathing* ist eine Technik, mit der Sie mehrere Elemente auf einem Pfad zur Übertragung von Daten zwischen dem ESX Server 3-Host und dem externen Speichergerät verwenden können. Bei Ausfall eines Elements im Pfad, eines HBA, eines Switches, eines Speicherprozessors (SP) oder Kabels kann ESX Server 3 einen redundanten Pfad verwenden. Der Prozess der Erkennung eines ausgefallenen Pfads und der Wechsel zu einem anderen Pfad wird als *Pfad-Failover* bezeichnet. Failover-Pfade stellen einen unterbrechungsfreien Datenverkehr zwischen dem ESX Server 3-System und den Speichergeräten sicher. Zur Multipathing-Unterstützung sind für ESX Server 3 keine speziellen Failover-Treiber erforderlich.

HINWEIS Eine virtuelle Maschine fällt auf nicht vorhersagbare Weise aus, wenn keiner der Pfade zum Speichergerät, auf dem die Festplatten der virtuellen Maschine gespeichert sind, zur Verfügung steht.

Der ESX Server 3-Host verwenden stets nur einen Pfad, den *aktiven Pfad*, um mit einem bestimmten Speichergerät zu einem beliebigen Zeitpunkt zu kommunizieren.

Bei der Auswahl des aktiven Pfads befolgt ESX Server 3 die folgenden Richtlinien für das Multipathing:

- **Zuletzt verwendet (Most Recently Used)** – Der ESX Server 3-Host wählt als aktiven Pfad den Pfad, der zuletzt verwendet wurde. Ist der Pfad nicht verfügbar, wechselt der Host zu einem anderen Pfad, um diesen als neuen aktiven Pfad zu nutzen.

  Die Richtlinie **Zuletzt verwendet (Most Recently Used)** ist für Speicherarrays vom Typ *Aktiv/Passiv* erforderlich, bei denen ein Speicherprozessor passiv bleibt und im Bedarfsfall aktiv wird.

- **Feststehend (Fixed)** – Der ESX Server 3-Host verwendet stets den vorgegebenen bevorzugten Pfad zum Speichergerät als aktiven Pfad. Wenn der ESX Server 3-Host nicht über diesen Pfad auf den Speicher zugreifen kann, wird ein anderer Pfad probiert, der anschließend zum aktiven Pfad wird. Sobald der bevorzugte Pfad wird verfügbar ist, kehrt der Host zu diesem zurück.

  VMware empfiehlt die Richtlinie **Feststehend (Fixed)** für Speicherarrays vom Typ *Aktiv/Aktiv*, bei denen alle Speicherprozessoren die Speicherdatenverkehr verarbeiten und alle Pfad stets aktiv sein können, es sei denn, ein Pfad fällt aus. Die meisten iSCSI-Speichersysteme sind vom Typ **Aktiv/Aktiv (active/active)**.

HINWEIS VMware empfiehlt nicht den manuellen Wechsel von **Zuletzt verwendet (Most Recently Used)** zu **Feststehend (Fixed)**. Das System stellt diese Richtlinie automatisch für die Arrays ein, für die diese Einstellung erforderlich ist.

- **Round Robin** – Der ESX Server 3-Host verwendet eine automatisch Rotation bei der Pfadauswahl unter Berücksichtigung aller verfügbaren Pfade. Zusätzlich zum Pfad-Failover unterstützt **Round Robin** den pfadübergreifenden Lastausgleich.

  In dieser Version ist der **Round Robin**-Lastausgleich experimentell und nicht für den Einsatz in Produktionsumgebungen vorgesehen. Siehe das Whitepaper zum *Round Robin-Lastausgleich*.

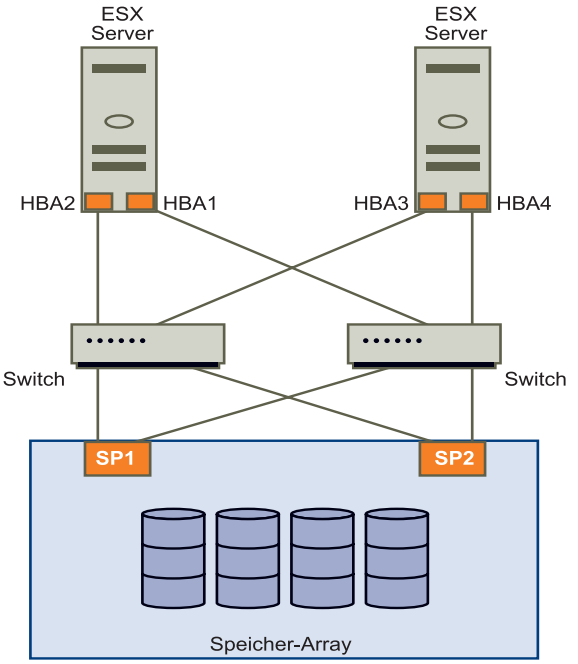
Multipathing mit lokalem Speicher und Fibre-Channel-SANs

Bei der einfachsten lokalen Speichertopologie für das Multipathing können Sie mit einem ESX Server 3-Host arbeiten, der über zwei HBAs verfügt. Der ESX Server 3-Host wird über zwei Kabel an das lokale Speichersystem mit zwei Ports angeschlossen. Bei dieser Konfiguration können Sie die Fehlertoleranz sicherstellen, sollte eines der Verbindungselemente zwischen dem ESX Server 3-Host und dem lokalen Speichersystem ausfallen.

Um Pfad-Switching mit Fibre-Channel-SAN zu unterstützen, verfügt der ESX Server 3-Host in der Regel über mindestens zwei HBAs, über die das Speicherarray unter Verwendung eines oder mehrerer Switches erreicht werden kann. Alternativ kann die Konfiguration auch einen HBA und zwei Speicherprozessoren aufweisen, sodass der HBA einen anderen Pfad verwenden kann, um auf das Festplatten-Array zuzugreifen.

Abbildung 7-1 zeigt, dass jeder Server über mehrere Pfade mit dem Speichergerät verbunden ist. Wenn zum Beispiel HBA1 oder die Verbindung zwischen HBA1 und dem Switch ausfällt, übernimmt HBA2 und stellt eine Verbindung zwischen dem Server und dem Switch zur Verfügung. Der Prozess, in dem ein HBA für einen anderen HBA einspringt, wird als HBA-Failover bezeichnet.

Abbildung 7-1. Fibre-Channel-Multipathing



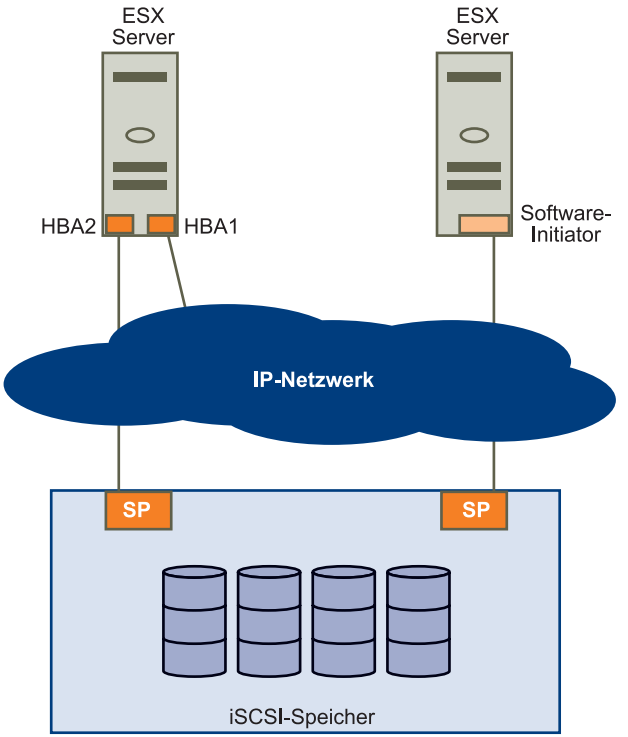
Analog dazu übernimmt SP2 bei einem Ausfall von SP1 oder der Verbindung zwischen SP1 und dem Switch und stellt eine Verbindung zwischen dem Switch und dem Speichergerät zur Verfügung. Dieser Vorgang wird SP-Failover genannt. VMware ESX Server 3 unterstützt über die Multipathing-Funktion sowohl das HBA- als auch das SP-Failover.

Siehe *SAN-Konfigurationshandbuch (für Fiber Channel)*.

Multipathing mit iSCSI-SAN

Bei der iSCSI-Speicherung nutzt ESX Server 3 die in das IP-Netzwerk integrierte Multipathing-Unterstützung, mit deren Hilfe das Netzwerk das Routing ausführen kann (siehe Abbildung 7-2). Über die dynamische Erkennung erhalten iSCSI-Initiatoren eine Liste mit Zieladressen, welche die Initiatoren als mehrere Pfade zu iSCSI-LUNs zu Failover-Zwecken nutzen können.

Abbildung 7-2. iSCSI-Multipathing



Zusätzlich zum Software-initiierten iSCSI können Sie mit der NIC-Gruppierung arbeiten, damit das Multipathing über die Netzwerkschicht im VMkernel erfolgt. Siehe „Netzwerk“ auf Seite 17.

Siehe *SAN-Konfigurationshandbuch (für iSCSI)*.

Anzeigen des aktiven Multipathing-Status

Verwenden Sie den VI-Client zum Anzeigen des aktuellen Multipathing-Status.

So zeigen Sie den aktuellen Multipathing-Status an

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

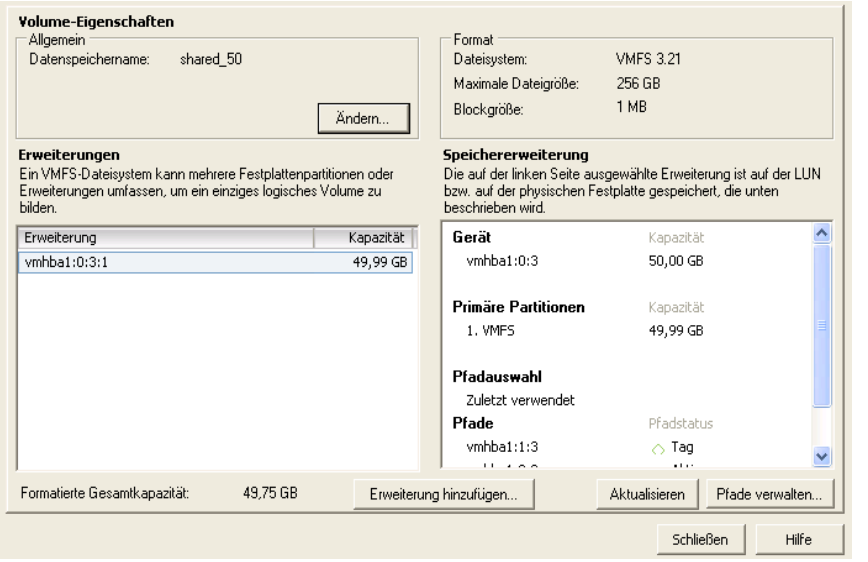
2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend unter **Hardware** auf **Speicher (Storage)**.

3 Wählen Sie in der Liste der konfigurierten Datenspeicher den Datenspeicher aus, dessen Pfade Sie anzeigen oder konfigurieren möchten.

Im Detailbereich werden alle Pfade angezeigt, über die auf den Datenspeicher zugegriffen wird, eingeschlossen der Status (aktiv, beschädigt oder deaktiviert).

4 Klicken Sie auf **Eigenschaften (Properties)**.

Das Dialogfeld **Volume-Eigenschaften (Volume Properties)** für den ausgewählten Datenspeicher wird geöffnet.



Unter **Gerät erweitern (Extent Device)** finden Sie Informationen zur Multipathing-Richtlinie, die der ESX Server 3-Host für den Zugriff auf den Datenspeicher verwendet, und zum Status der einzelnen Pfade angezeigt. Die folgenden Pfadinformationen werden ggf. angezeigt:

- **Aktiv (Active)** – Der Pfad ist aktiv und ist der aktuell verwendete Pfad für die Übermittlung von Daten.
- **Deaktiviert (Disabled)** – Der Pfad wurde deaktiviert, sodass keine Daten übertragen werden können.
- **Standby** – Der Pfad funktioniert, wird jedoch derzeit nicht zum Übertragen von Daten verwendet.
- **Beschädigt (Broken)** – Die Software kann über diesen Pfad keine Verbindung mit der Festplatte herstellen.

5 Klicken Sie auf **Pfade verwalten (Manage Paths)**, um das Dialogfeld **Pfade verwalten (Manage Paths)** zu öffnen.

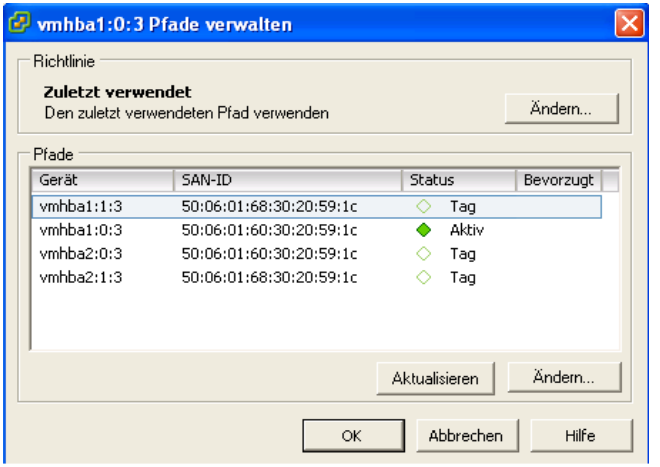
Wenn Sie die Pfadrichtlinie **Feststehend (Fixed)** verwenden, können Sie erkennen, welcher Pfad der bevorzugte Pfad ist. Der bevorzugte Pfad ist mit einem Sternchen (*) in der vierten Spalte gekennzeichnet.

Sie können das Dialogfeld **Pfade verwalten (Manage Paths)** verwenden, um die Pfade zu aktivieren oder zu deaktivieren, die Multipathing-Richtlinie zu konfigurieren oder den bevorzugten Pfad anzugeben.

Einrichten von Multipathing-Richtlinien für LUNs

Im Dialogfeld **Pfade verwalten (Manage Paths)** können Sie die Multipathing-Richtlinie festlegen und den bevorzugten Pfad für die Richtlinie **Feststehend (Fixed)** angeben. Wenn Sie Pfade für Raw-Gerätezuordnungen verwalten, finden Sie weitere Informationen unter „So verwalten Sie Pfade“ auf Seite 168.

Das Dialogfeld **Pfade verwalten (Manage Paths)** enthält eine Liste mit verschiedenen Pfaden zur Festplatte sowie die Multipathing-Richtlinie für die Festplatte und den Verbindungsstatus für jeden einzelnen Pfad. Sie zeigt außerdem den bevorzugten Pfad zu der Festplatte an.



So richten Sie die Multipathing-Richtlinie ein

1 Klicken Sie unter **Richtlinie (Policy)** auf **Ändern (Change)**.

2 Wählen Sie eine der folgenden Optionen aus:

- **Feststehend (Fixed)**
- **Zuletzt verwendet (Most Recently Used)**
- **Round Robin (Experimentell)**

3 Klicken Sie auf **OK** und dann auf **Schließen (Close)**, um die Einstellungen zu speichern und zur Seite **Konfiguration (Configuration)** zurückzukehren.

HINWEIS VMware empfiehlt die Richtlinie **Zuletzt verwendet (Most Recently Used)** für Aktiv/Passiv-Speichergeräte.

Wenn Sie die Pfadrichtlinie auf **Feststehend (Fixed)** festlegen, geben Sie den bevorzugten Pfad an, den der Host, falls verfügbar, verwenden soll.

So richten Sie den bevorzugten Pfad ein

1 Wählen Sie unter **Pfade (Paths)** den Pfad aus, der der bevorzugte Pfad werden soll, und klicken Sie anschließend auf **Ändern (Change)**.

2 Klicken Sie im Bereich **Einstellungen (Preference)** auf **Bevorzugt (Preferred)**.

Wenn die Option **Bevorzugt (Preferred)** nicht verfügbar ist, stellen Sie sicher, dass die **Pfadrichtlinie (Path Policy)** auf **Feststehend (Fixed)** festgelegt ist.

3 Klicken Sie zweimal auf **OK**, um Ihre Einstellungen zu speichern und die Dialogfelder zu schließen.

Deaktivieren von Pfaden

Im VI-Client können Sie Pfade aus Wartungs- und anderen Gründen vorübergehend deaktivieren.

So deaktivieren Sie einen Pfad

1 Wählen Sie unter **Pfade (Paths)** den Pfad aus, den Sie deaktivieren möchten, und klicken Sie anschließend auf **Ändern (Change)**.

2 Wählen Sie **Deaktivieren (Disabled)** aus, um den Pfad zu deaktivieren.

3 Klicken Sie zweimal auf **OK**, um Ihre Einstellungen zu speichern und die Dialogfelder zu schließen.

Die vmkfstools-Befehle

Zusätzlich zum VI-Client können Sie das Dienstprogramm `vmkfstools` einsetzen, um physische Speichergeräte zu verwalten und VMFS-Datenspeicher und -Volumes auf Ihrem ESX Server 3-Host zu erstellen und zu bearbeiten.

Eine Liste unterstützter `vmkfstools`-Befehle finden Sie unter „Verwenden von „vmkfstools““ auf Seite 299.

Raw-Gerätezuordnung 8

Die Raw-Gerätezuordnung bietet virtuellen Maschinen einen Mechanismus für den direkten Zugriff auf eine LUN im physischen Speichersubsystem (nur Fibre-Channel oder iSCSI). Dieses Kapitel enthält Informationen zu Raw-Gerätezuordnungen.

In diesem Kapitel werden folgende Themen behandelt:

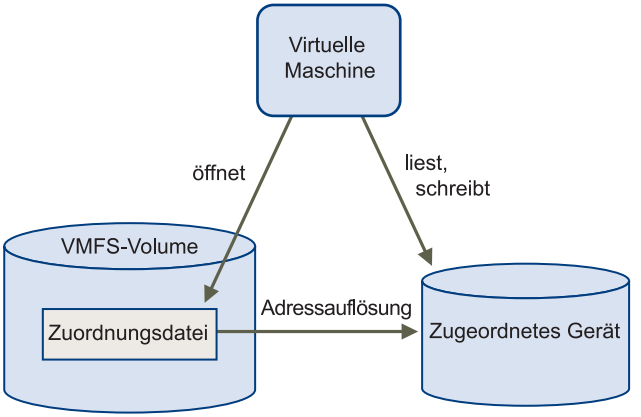
- „Wissenswertes zur Raw-Gerätezuordnung“ auf Seite 156
- „Raw-Gerätezuordnungseigenschaften“ auf Seite 161
- „Verwalten zugeordneter LUNs“ auf Seite 165

Wissenswertes zur Raw-Gerätezuordnung

Zur Raw-Gerätezuordnung gehört eine Zuordnungsdatei in einem getrennten VMFS-Volume, die als Stellvertreter für ein physisches Raw-Gerät fungiert, das direkt von einer virtuellen Maschine verwendet wird. Die Raw-Gerätezuordnungsdatei enthält Metadaten, mit denen Festplattenzugriffe auf das physische Gerät verwaltet und umgeleitet werden. Die Datei bietet Ihnen einige der Vorteile des direkten Zugriffs auf ein physisches Gerät, während Sie gleichzeitig verschiedene Vorteile einer virtuellen Festplatte im VMFS-Dateisystem nutzen können. Folglich verbindet die Datei die VMFS-Verwaltungs- und Wartungsfreundlichkeit mit einem Raw-Gerätezugriff.

Raw-Gerätezuordnungen können beispielsweise wie folgt beschrieben werden: „Zuordnen eines Raw-Geräts zu einem Datenspeicher“, „Zuordnen einer System-LUN“ oder „Zuordnen einer Festplattendatei zu einem physischen Festplatten-Volume“. All diese Zuordnungsbegriffe beziehen sich auf Raw-Gerätezuordnungen.

Abbildung 8-1. Raw-Gerätezuordnung



Obwohl VMFS für die meisten virtuellen Festplattenspeicher von VMware empfohlen wird, kann es in Einzelfällen erforderlich sein, Raw-LUNs oder logische Festplatten in einem SAN zu verwenden.

So ist es beispielsweise in folgenden Situationen erforderlich, Raw-LUNs zusammen mit zu Raw-Gerätezuordnungen zu verwenden:

- Wenn in der virtuellen Maschine ein SAN-Snapshot oder auf Ebenen basierende Anwendungen ausgeführt werden. Die Raw-Gerätezuordnung unterstützt Systeme zur Auslagerung von Datensicherungen, indem SAN-eigene Funktionen verwendet werden.

- In allen MSCS-Clusterszenarien, die sich über mehrere physische Hosts erstrecken (in Virtuell-zu-Virtuell-Clustern und in Physisch-zu-Virtuell-Clustern). In diesem Fall sollten Clusterdaten und Quorumfestplatten vorzugsweise als Raw-Gerätezuordnungen konfiguriert werden und nicht als Dateien auf einem freigegebenen VMFS.

Stellen Sie sich eine Raw-Gerätezuordnung als eine symbolische Verknüpfung zwischen einem VMFS-Volume und einer Raw-LUN vor (siehe Abbildung 8-1). Die Zuordnung zeigt die LUNs wie Dateien auf einem VMFS-Volume an. In der Konfiguration der virtuellen Maschine wird auf die Raw-Gerätezuordnung und nicht auf die Raw-LUN verwiesen. Die Raw-Gerätezuordnung enthält einen Verweis auf die Raw-LUN.

Mithilfe von Raw-Gerätezuordnungen ist Folgendes möglich:

- Migrieren virtueller Maschinen mit VMotion über Raw-LUNs.
- Hinzufügen von Raw-LUNs zu virtuellen Maschinen mithilfe des VI-Clients.
- Verwenden von Dateisystemfunktionen wie verteilte Dateisperrung, Berechtigungen und Benennung.

Für Raw-Gerätezuordnungen gibt es zwei Kompatibilitätsmodi:

- Mit dem Modus „Virtuelle Kompatibilität“ kann sich eine Raw-Gerätezuordnung ebenso wie eine virtuelle Festplattendatei verhalten. Dies umfasst auch die Verwendung von Snapshots.
- Im Modus „Physische Kompatibilität“ können Anwendungen, die eine hardwarenähere Steuerung benötigen, direkt auf das SCSI-Gerät zugreifen.

Vorteile von Raw-Gerätezuordnungen

Eine Raw-Gerätezuordnung bietet mehrere Vorteile, sollte aber nicht ständig verwendet werden. In der Regel sind virtuelle Festplattendateien aufgrund ihrer Verwaltungsfreundlichkeit Raw-Gerätezuordnungen vorzuziehen. Wenn Sie jedoch Raw-Geräte benötigen, müssen Sie die Raw-Gerätezuordnung verwenden. In der folgenden Liste sind die Vorteile der Raw-Gerätezuordnung zusammengefasst:

- **Benutzerfreundliche, dauerhafte Namen** – Die Raw-Gerätezuordnung ermöglicht benutzerfreundliche Namen für zugeordnete Geräte. Wenn Sie eine Raw-Gerätezuordnung verwenden, müssen Sie nicht auf das Gerät über den Gerätenamen verweisen. Sie verwenden stattdessen den Namen der Zuordnungsdatei, zum Beispiel:

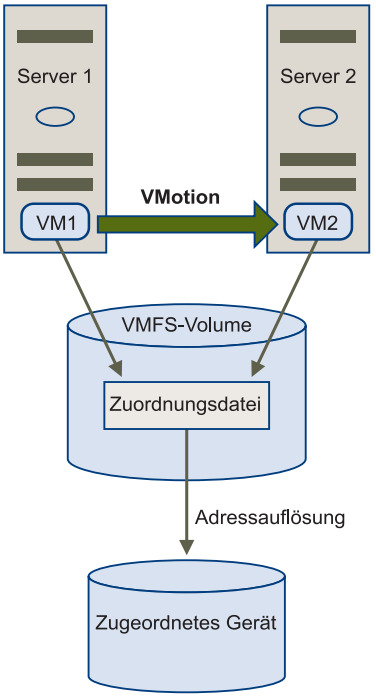
  ```
  /vmfs/volumes/myVolume/myVMDirectory/myRawDisk.vmdk
  ```

- **Dynamische Namensauflösung** – Die Raw-Gerätezuordnung speichert eindeutige Identifikationsdaten für jedes zugeordnete Gerät. Das VMFS-Dateisystem ordnet jede Raw-Gerätezuordnung unabhängig von Änderungen der physischen Konfiguration des Servers aufgrund von Änderungen an der Adapterhardware, Verzeichniswechseln, Geräteverschiebungen usw. Ihrem aktuellen SCSI-Gerät zu.
- **Verteilte Dateisperrung** – Die Raw-Gerätezuordnung ermöglicht die Verwendung einer verteilten VMFS-Sperrung für Raw-SCSI-Geräte. Die verteilte Sperrung für eine Raw-Gerätezuordnung ermöglicht die Verwendung einer freigegebenen Raw-LUN ohne Datenverlustrisiko, wenn zwei virtuelle Maschinen auf verschiedenen Servern versuchen, auf die gleiche LUN zuzugreifen.
- **Dateizugriffsberechtigungen** – Die Raw-Gerätezuordnung ermöglicht Dateizugriffsberechtigungen. Die Berechtigungen für die Zuordnungsdatei werden beim Öffnen der Datei erzwungen, um das zugeordnete Volume zu schützen.
- **Dateisystemoperationen** – Die Raw-Gerätezuordnung ermöglicht bei der Arbeit mit einem zugeordneten Volume die Verwendung von Dienstprogrammen des Dateisystems, wobei die Zuordnungsdatei als Stellvertreter verwendet wird. Die meisten Vorgänge, die auf eine normale Datei angewendet werden können, können auf die Zuordnungsdatei angewendet werden und werden dann auf das zugeordnete Gerät umgeleitet.
- **Snapshots** – Die Raw-Gerätezuordnung ermöglicht die Verwendung von Snapshots virtueller Maschinen auf einem zugeordneten Volume.

  HINWEIS Snapshots stehen nicht zur Verfügung, wenn die Raw-Gerätezuordnung im Modus „Physische Kompatibilität“ verwendet wird.

- **VMotion** – Mithilfe der Raw-Gerätezuordnung können Sie eine virtuelle Maschine mit VMotion migrieren. Die Zuordnungsdatei fungiert als Stellvertreter, sodass VirtualCenter die virtuelle Maschine mit dem gleichen Mechanismus migrieren kann, der für die Migration virtueller Festplattendateien verwendet wird. Siehe Abbildung 8-2.

Abbildung 8-2. VMotion einer virtuellen Maschine über eine Raw-Gerätezuordnung



- **SAN-Verwaltungs-Agenten** – Die Raw-Gerätezuordnung ermöglicht die Ausführung bestimmter SAN-Verwaltungs-Agenten innerhalb einer virtuellen Maschine. Außerdem kann jede Software, die Zugriff auf ein Gerät über hardwarespezifische SCSI-Befehle benötigt, in einer virtuellen Maschine ausgeführt werden. Diese Art der Software wird auch SCSI-Ziel-basierte Software genannt.

  HINWEIS Wenn Sie SAN-Verwaltungs-Agenten verwenden, müssen Sie den physischen Kompatibilitätsmodus für die Raw-Gerätezuordnung auswählen.

- **N-Port-ID-Virtualisierung (NPIV)** – Ermöglicht den Einsatz der NPIV-Technologie, die es einem einzelnen Fibre-Channel-HBA-Port ermöglicht, sich mit dem Fibre-Channel-Fabric über mehrere WWPNs (Worldwide Port Names) zu verbinden. Dadurch kann der HBA-Port in Form mehrerer virtueller Ports angezeigt werden, die alle über eine eigene ID und einen eigenen virtuellen Portnamen verfügen. Virtuelle Maschinen können anschließend jeden dieser virtuellen Ports beanspruchen und für den gesamten zur Raw-Gerätezuordnung gehörenden Datenverkehr nutzen.

  HINWEIS NPIV wird nur für virtuelle Maschinen mit Raw-Gerätezuordnungsfestplatten unterstützt.

  Siehe *SAN-Konfigurationshandbuch (für Fiber Channel)*.

VMware kooperiert mit Anbietern von Speicherverwaltungssoftware, damit deren Software in Umgebungen wie ESX Server 3 ordnungsgemäß funktioniert. Beispiele sind:

- SAN-Verwaltungssoftware
- Software zur Verwaltung von Speicherressourcen
- Snapshot-Software
- Replikationssoftware

Diese Software verwendet für Raw-Gerätezuordnungen den Modus „Physische Kompatibilität“, damit sie direkt auf SCSI-Geräte zugreifen kann.

Verschiedene Verwaltungsprodukte werden besser zentral (nicht auf dem ESX Server 3-Computer) ausgeführt, während andere problemlos in der Servicekonsole oder in den virtuellen Maschinen funktionieren. VMware zertifiziert diese Anwendungen nicht und stellt auch keine Kompatibilitätsmatrix zur Verfügung. Wenn Sie wissen möchten, ob eine SAN-Verwaltungsanwendung in einer ESX Server 3-Umgebung unterstützt wird, wenden Sie sich an den Hersteller.

Einschränkungen der Raw-Gerätezuordnung

Beachten Sie Folgendes, wenn Sie die Raw-Gerätezuordnung verwenden möchten:

- **Nicht verfügbar für Block- und bestimmte RAID-Geräte** – Die Raw-Gerätezuordnung (in der gegenwärtigen Implementierung) verwendet zur Identifizierung des zugeordneten Geräts eine SCSI-Seriennummer. Da Block- und bestimmte direkt angeschlossene RAID-Geräte Seriennummern nicht exportieren, können sie nicht in Raw-Gerätezuordnungen verwendet werden.
- **Nur für Volumes mit VMFS-2 und VMFS-3** – Die Raw-Gerätezuordnung erfordert das Format VMFS-2 oder VMFS-3. Unter ESX Server 3 ist das Dateisystem VMFS-2 schreibgeschützt. Aktualisieren Sie es auf VMFS-3, um die in VMFS-2 gespeicherten Dateien nutzen zu können.
- **Keine Snapshots im Modus „Physische Kompatibilität“** – Wenn Sie die Raw-Gerätezuordnung im Modus „Physische Kompatibilität“ verwenden, können Sie für die Festplatte keine Snapshots verwenden. Im Modus „Physische Kompatibilität“ kann die virtuelle Maschine eigene Snapshots oder Spiegelungsoperationen durchführen.

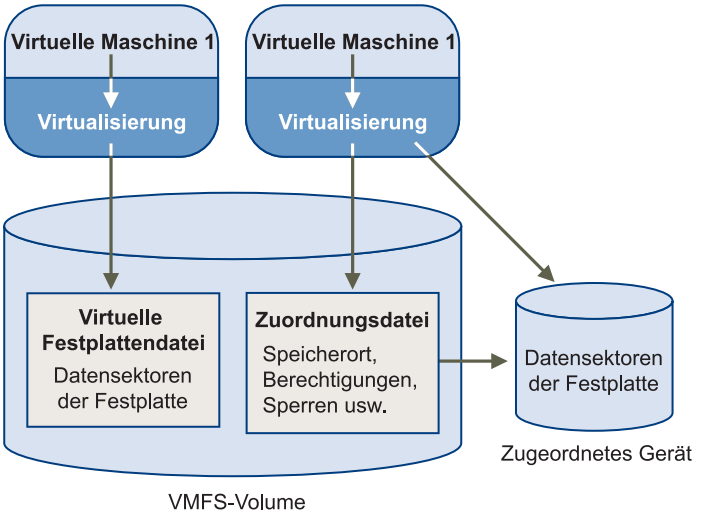
  Im Modus „Virtuelle Kompatibilität“ stehen dagegen Snapshots zur Verfügung. Siehe „Vergleich des virtuellen und mit dem physischen Kompatibilitätsmodus“ auf Seite 161.
- **Keine Partitionszuordnung** – Für die Raw-Gerätezuordnung muss das zugeordnete Gerät eine vollständige LUN sein. Die Zuordnung zu einer Partition wird nicht unterstützt.

Raw-Gerätezuordnungseigenschaften

Eine Raw-Gerätezuordnung ist eine spezielle Datei auf einem VMFS-Volume, mit deren Hilfe die Metadaten für das zugeordnete Gerät verwaltet werden. Die Verwaltungssoftware erkennt die Zuordnungsdatei als normale Festplattendatei, die für normale Dateisystemoperationen zur Verfügung steht. Die virtuelle Maschine erkennt das zugeordnete Gerät aufgrund der Speichervirtualisierungsebene als virtuelles SCSI-Gerät.

Zu den wichtigsten Metadaten in der Zuordnungsdatei gehören der Speicherort (Namensauflösung) und der Sperrstatus des zugeordneten Geräts.

Abbildung 8-3. Metadaten der Zuordnungsdatei

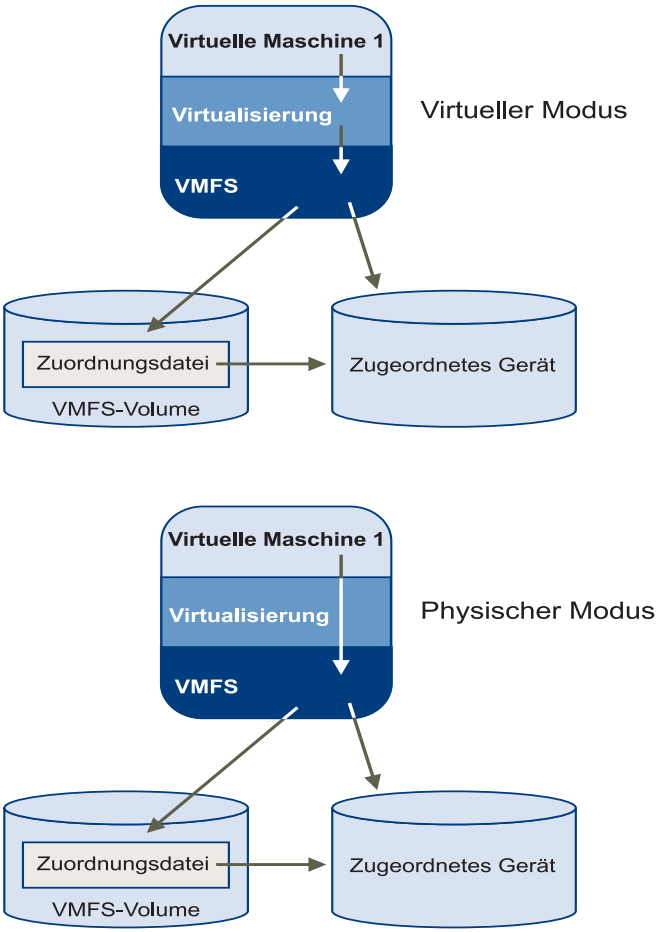


Vergleich des virtuellen und mit dem physischen Kompatibilitätsmodus

Der virtuelle Modus für eine Raw-Gerätezuordnung legt die vollständige Virtualisierung des zugeordneten Geräts fest. Das Gastbetriebssystem erkennt keinen Unterschied zwischen einem zugeordneten Gerät und einer virtuellen Festplattendatei auf einem VMFS-Volume. Die tatsächlichen Hardwaremerkmale sind verborgen. Mit dem virtuellen Modus können Kunden, die Raw-Festplatten verwenden, die Vorteile von VMFS, z. B. leistungsfähige Dateisperrung zum Datenschutz und Snapshots zur Vereinfachung von Entwicklungsprozessen, nutzen. Der virtuelle Modus ist auch besser zwischen Speichergeräten portierbar als der physische Modus, da er das gleiche Verhalten wie virtuelle Festplattendateien aufweist.

Der physische Modus einer Raw-Gerätezuordnung legt eine minimale SCSI-Virtualisierung des zugeordneten Geräts fest, wodurch eine optimale Flexibilität der SAN-Verwaltungssoftware erreicht wird. Im physischen Modus leitet der VMkernel alle SCSI-Befehle bis auf eine Ausnahme an das Gerät weiter: Der Befehl **REPORT LUNs** ist virtualisiert, damit der VMkernel die LUN für die entsprechende virtuelle Maschine isolieren kann. Ansonsten sind alle physischen Charakteristika der zu Grunde liegenden Hardware sichtbar. Der physische Modus ist für die Ausführung von SAN-Verwaltungs-Agenten oder anderer SCSI-Ziel-basierter Software in der virtuellen Maschine bestimmt. Der physische Modus ermöglicht auch zum kostengünstigen Erzielen einer hohen Verfügbarkeit die Bildung von VM-PC-Clustern.

Abbildung 8-4. Die Modi „Virtuelle Kompatibilität“ und „Physische Kompatibilität“

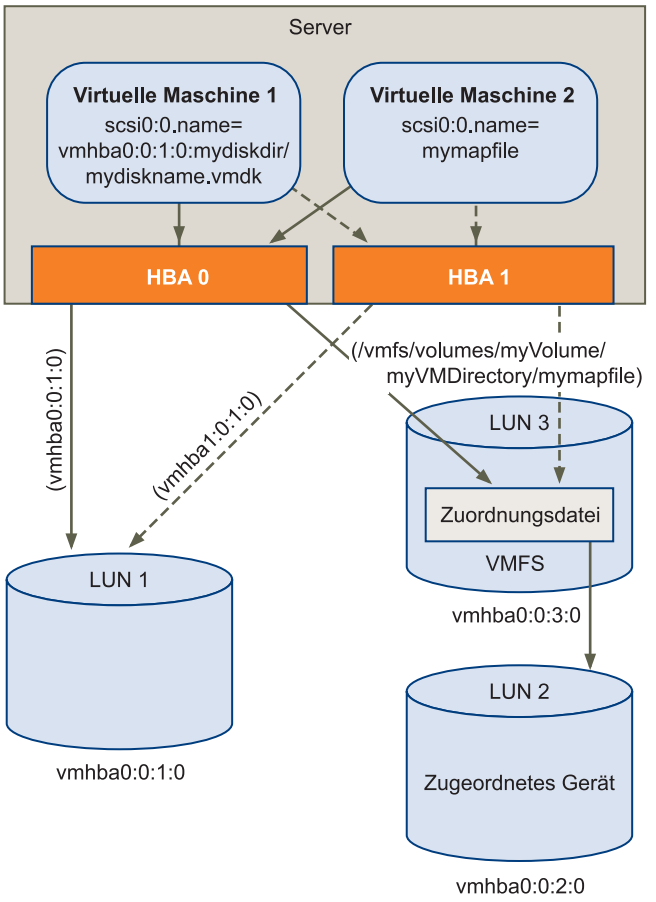


Dynamische Namensauflösung

Mit der Raw-Gerätezuordnung können Sie einem Gerät einen dauerhaften Namen geben, indem Sie auf den Namen der Zuordnungsdatei im Unterverzeichnis `/vmfs` verweisen.

Das Beispiel in Abbildung 8-5 zeigt drei LUNs. Auf LUN 1 wird über den Gerätenamen zugegriffen, der von der ersten sichtbaren LUN abhängt. LUN 2 ist ein zugeordnetes Gerät, das von einer Raw-Gerätezuordnung auf LUN 3 verwaltet wird. Der Zugriff auf die Raw-Gerätezuordnung erfolgt über den feststehenden Pfadnamen im Unterverzeichnis `/vmfs`.

Abbildung 8-5. Beispiel einer Namensauflösung

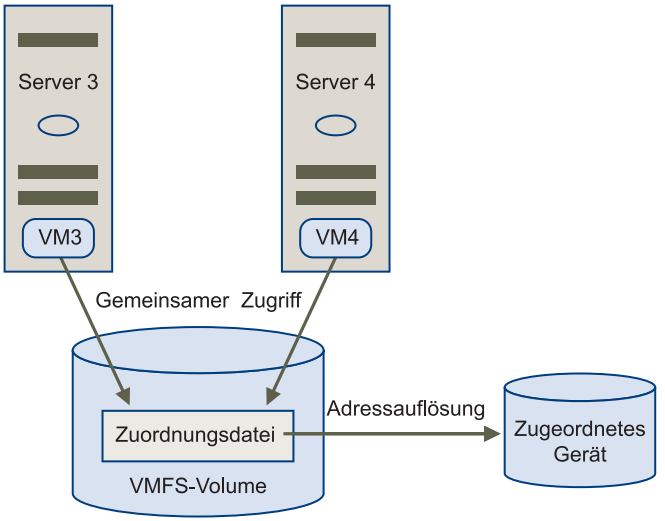


Alle zugeordneten LUNs werden durch VMFS eindeutig bezeichnet. Die Bezeichnung wird in den internen LUN-Datenstrukturen gespeichert. Jede Änderung des SCSI-Pfads (z. B. Ausfall eines Fibre-Channel-Switches oder Hinzufügung eines neuen Host-Bus-Adapters) kann zu einer Änderung des „vmhba“-Gerätenamens führen, da zum Namen auch die Pfadangabe (Ursprung, Ziel, LUN) gehört. Die dynamische Namensauflösung gleicht diese Änderungen durch die Anpassung der Datenstrukturen aus, wodurch die LUNs auf die neuen Gerätenamen umgeleitet werden.

Raw-Gerätezuordnung für Cluster aus virtuellen Maschinen

Die Verwendung einer Raw-Gerätezuordnung ist für Cluster mit virtuellen Maschinen erforderlich, die zur Sicherstellung von Failover auf die gleiche Raw-LUN zugreifen müssen. Die Einrichtung ist vergleichbar mit der Einrichtung eines solchen Clusters mit Zugriff auf dieselbe virtuelle Festplattendatei. Die virtuelle Festplattendatei wird dabei allerdings durch die Raw-Gerätezuordnung ersetzt.

Abbildung 8-6. Zugriff aus virtuellen Maschinen in Clustern



Weitere Informationen finden Sie im *Handbuch zur Ressourcenverwaltung*.

Vergleich der Raw-Gerätezuordnung mit anderen Möglichkeiten des SCSI-Gerätezugriffs

Um die Entscheidung zwischen den verschiedenen verfügbaren Zugriffsmodi für SCSI-Geräte zu erleichtern, bietet Tabelle 8-1 einen Vergleich der Funktionen in den verschiedenen Modi.

Tabelle 8-1. Verfügbare Funktionen bei virtuellen Festplatten und Raw-Gerätezuordnungen

ESX Server 3 - Funktionen	Virtuelle Festplattendatei	Raw-Gerätezuordnung - Virtueller Modus	Raw-Gerätezuordnung - Physischer Modus
Weitergabe von SCSI-Befehlen	Nein	Nein	Ja Der Befehl REPORT LUNs wird nicht weitergegeben
Unterstützung von VirtualCenter	Ja	Ja	Ja
Snapshots	Ja	Ja	Nein
Verteilte Sperrung	Ja	Ja	Ja
Clusterbildung	Nur systeminterne Cluster	Systeminterne und systemübergreifende Cluster	N+1 (nur VM/PC-Cluster)
SCSI-Ziel-basierte Software	Nein	Nein	Ja

VMware empfiehlt für systeminterne Cluster den Einsatz virtueller Festplattendateien. Wenn Sie systeminterne Cluster als systemübergreifende Cluster rekonfigurieren möchten, verwenden Sie für systeminterne Cluster Raw-Gerätezuordnungen. Weitere Informationen finden Sie im *Handbuch zur Ressourcenverwaltung*.

Verwalten zugeordneter LUNs

Zu den Werkzeugen, die für die Verwaltung zugeordneter LUNs und ihrer Raw-Gerätezuordnungen verfügbar sind, gehören der VI-Client von VMware, das Dienstprogramm `vmkfstools` und die normalen Dienstprogramme des Dateisystems, die in der Servicekonsole verwendet werden.

VMware Infrastructure-Client

Mithilfe des VI-Clients können Sie eine SAN-LUN einem Datenspeicher zuordnen und Pfade zur zugeordneten LUN verwalten.

Erstellen virtueller Maschinen mit Raw-Gerätezuordnungen

Wenn Sie eine virtuelle Maschine mit einem Direktzugriff auf eine Raw-SAN-LUN versehen, erstellen Sie eine Zuordnungsdatei (Raw-Gerätezuordnung), die sich in einem VMFS-Datenspeicher befindet und auf die LUN verweist. Wenngleich die Zuordnungsdatei dieselbe `.vmdk`-Erweiterung wie eine herkömmliche virtuelle Festplattendatei hat, enthält die Raw-Gerätezuordnungsdatei nur Zuordnungsinformationen. Die eigentlichen virtuellen Festplattendaten werden direkt in der LUN gespeichert.

Sie können die Raw-Gerätezuordnung als Ausgangsfestplatte für eine neue virtuelle Maschine erstellen oder sie einer vorhandenen virtuellen Maschine hinzufügen. Beim Erstellen der Raw-Gerätezuordnung geben Sie die zuzuordnende LUN und den Datenspeicher an, in dem die Raw-Gerätezuordnung abgelegt werden soll.

So erstellen Sie eine virtuelle Maschine mit einer Raw-Gerätezuordnung

1 Befolgen Sie sämtliche Anweisungen zum Erstellen einer benutzerdefinierten virtuellen Maschine.

Siehe *Grundlegende Systemverwaltung*.

2 Wählen Sie auf der Seite **Festplatte auswählen (Select a Disk)** die Option **Raw-Gerätezuordnung (Raw Device Mapping)** aus, und klicken Sie anschließend auf **Weiter (Next)**.

3 Wählen Sie in der Liste der SAN-Festplatten bzw. LUNs eine Raw-LUN auf, auf welche die virtuelle Maschine direkt zugreifen soll.

Weitere Informationen zum Konfigurieren von SAN-Speicher finden Sie im *SAN-Konfigurationshandbuch (für Fiber Channel)* und im *SAN-Konfigurationshandbuch (für iSCSI)*.

4 Wählen Sie einen Datenspeicher für die Raw-Gerätezuordnungsdatei aus.

Sie können die Raw-Gerätezuordnungsdatei im selben Datenspeicher ablegen, in dem sich die Konfigurationsdatei der virtuellen Maschine befindet, oder einen anderen Datenspeicher auswählen.

HINWEIS Um VMotion für virtuelle Maschinen mit aktivierter NPIV zu verwenden, müssen sich die Raw-Gerätezuordnungsdateien der virtuellen Maschinen im selben Datenspeicher befinden. Bei aktivierter NPIV ist Storage VMotion bzw. VMotion zwischen Datenspeichern nicht möglich.

---

5 Wählen Sie den Kompatibilitätsmodus aus:

- Im **physischen Kompatibilitätsmodus (Physical compatibility)** kann das Gastbetriebssystem direkt auf die Hardware zugreifen. Der physische Kompatibilitätsmodus bietet sich an, wenn Sie SAN-fähige Anwendungen in der virtuellen Maschine einsetzen. Eine virtuelle Maschine, die für den physischen Kompatibilitätsmodus für die Raw-Gerätezuordnung konfiguriert ist, kann jedoch weder geklont noch in eine Vorlage umgewandelt noch migriert werden, wenn für die Migration die Festplatte kopiert werden muss.
- Im **virtuellen Kompatibilitätsmodus (Virtual compatibility)** kann sich die Raw-Gerätezuordnung wie eine virtuelle Festplatte verhalten, sodass Sie Funktionen wie Snapshots, Klonen usw. verwenden können.

6 Wählen Sie den Knoten des virtuellen Geräts aus.

7 Wenn Sie **Unabhängiger Modus (Independent)** wählen, aktivieren Sie eine der folgenden Optionen:

- **Dauerhaft (Persistent)** – Änderungen werden sofort und permanent auf die Festplatte geschrieben.
- **Nicht-dauerhaft (Nonpersistent)** – Auf die Festplatte geschriebene Änderungen werden beim Herunterfahren oder Wiederherstellen eines Snapshots verworfen.

8 Klicken Sie auf **Weiter (Next)**.

9 Überprüfen Sie auf der Seite **Bereit zum Abschließen der neuen virtuellen Maschine (Ready to Complete New Virtual Machine)** Ihre Angaben.

10 Klicken Sie auf **Fertig (Finish)**, um die virtuelle Maschine zu erstellen.

Sie können eine Raw-Gerätezuordnung auch einer vorhandenen virtuellen Maschine hinzufügen.

So fügen Sie eine Raw-Gerätezuordnung zu einer virtuellen Maschine hinzu

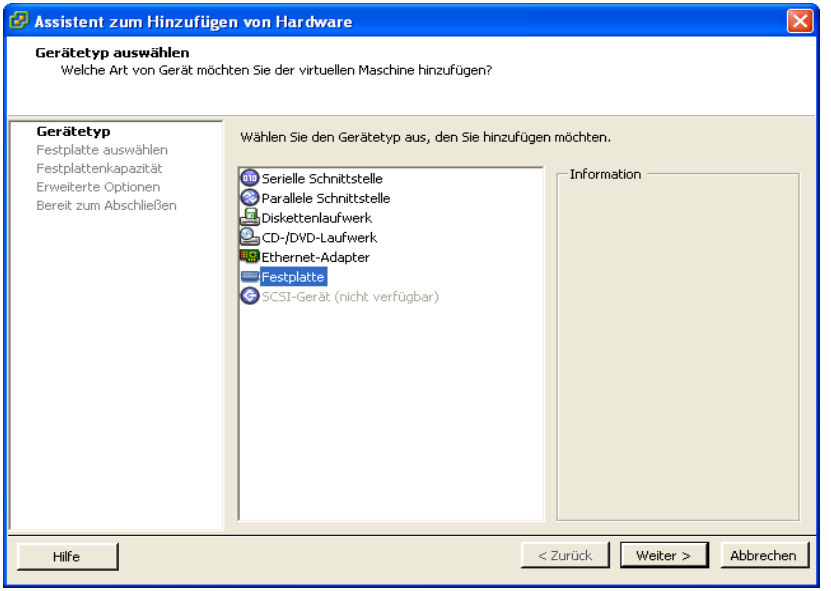
1 Klicken Sie im VI-Client in der Navigationsleiste auf **Bestandsliste (Inventory)**, und erweitern Sie die Liste bei Bedarf.

2 Wählen Sie die virtuelle Maschine in der Bestandsliste aus.

3 Klicken Sie auf der Registerkarte **Übersicht (Summary)** auf **Einstellungen bearbeiten (Edit Settings)**.

4 Klicken Sie auf **Hinzufügen (Add)**.

Der Assistent zum Hinzufügen von Hardware wird geöffnet.



5 Wählen Sie als Gerät, das hinzugefügt werden soll, **Festplatte (Hard Disk)** aus, und klicken Sie auf **Weiter (Next)**.

6 Wählen Sie **Raw-Gerätezuordnung (Raw Device Mapping)**, und klicken Sie auf **Weiter (Next)**.

7 Informationen zur Vorgehensweise finden Sie unter Schritt 3.

Verwalten von Pfaden für eine zugeordnete Raw-LUN

Sie können im Dialogfeld **Pfade verwalten (Manage Paths)** die Pfade Ihrer Zuordnungsdateien und zugeordneten Raw-LUNs verwalten.

So verwalten Sie Pfade

1 Melden Sie sich als Administrator oder als Besitzer der virtuellen Maschine an, zu der die zugeordnete Festplatte gehören soll.

2 Wählen Sie die virtuelle Maschine in der Bestandsliste aus.

3 Klicken Sie auf der Registerkarte **Übersicht (Summary)** auf **Einstellungen bearbeiten (Edit Settings)**.

Das Dialogfeld **Eigenschaften der virtuellen Maschinen (Virtual Machine Properties)** wird geöffnet.

4 Klicken Sie auf der **Hardware** auf **Festplatte (Hard Disk)** und dann auf **Pfade verwalten (Manage Paths)**.

5 Im Dialogfeld **Pfade verwalten (Manage Paths)** können Sie Ihre Pfade aktivieren oder deaktivieren, eine Multipathing-Richtlinie festlegen und den bevorzugten Pfad angeben.

Folgen Sie den folgenden Vorgehensweisen:

- „So richten Sie die Multipathing-Richtlinie ein“ auf Seite 152
- „So richten Sie den bevorzugten Pfad ein“ auf Seite 153
- „So deaktivieren Sie einen Pfad“ auf Seite 153

Das Dienstprogramm vmkfstools

In der Servicekonsole kann für viele der Operationen, die über den VI-Client ausgeführt werden, das Befehlszeilendienstprogramm `vmkfstools` verwendet werden. Zu den typischen Operationen für die Raw-Gerätezuordnung gehören die Befehle zur Erstellung einer Zuordnungsdatei, die Abfrage von Zuordnungsinformationen wie Name und Bezeichnung des zugeordneten Geräts und Import und Export einer virtuellen Festplatte.

Siehe „Verwenden von „vmkfstools““ auf Seite 299.

Dateisystemfunktionen

Die meisten Dateisystemfunktionen, die in der Servicekonsole ausgeführt werden können, können auf Raw-Gerätezuordnungen angewendet werden.

Tabelle 8-2. In der Servicekonsole aufgerufene Befehle

Befehl	Beschreibung
`ls -l`	Zeigt den Datennamen und die Zugriffsberechtigungen der Zuordnungsdatei sowie die Länge des zugeordneten Geräts.
`du`	Zeigt den vom zugeordneten Gerät belegten Speicherplatz, jedoch nicht die Zuordnungsdatei an.
`mv`	Benennt die Zuordnungsdatei um, ohne das zugeordnete Gerät zu beeinflussen.
`cp`	Kopiert den Inhalt eines zugeordneten Geräts. Sie können eine virtuelle Festplattendatei nicht auf ein zugeordnetes Gerät kopieren. Verwenden Sie statt dessen den Befehl `vmkfstools`.
`dd`	Kopiert Datei auf oder von einem zugeordneten Gerät. VMware empfiehlt Ihnen, die Import- und Export-Befehle in `vmkfstools` zu verwenden.

Sicherheit

Sicherheit für ESX Server 3-Systeme

9

Bei der Entwicklung von ESX Server war hohe Sicherheit einer der Schwerpunkte. Dieser Abschnitt bietet Ihnen eine Übersicht darüber, wie VMware Sicherheit in der ESX Server Umgebung gewährleistet. Dies erfolgt insbesondere über die Sicherheitsaspekte der Systemarchitektur und eine Liste zusätzlicher Sicherheitsressourcen.

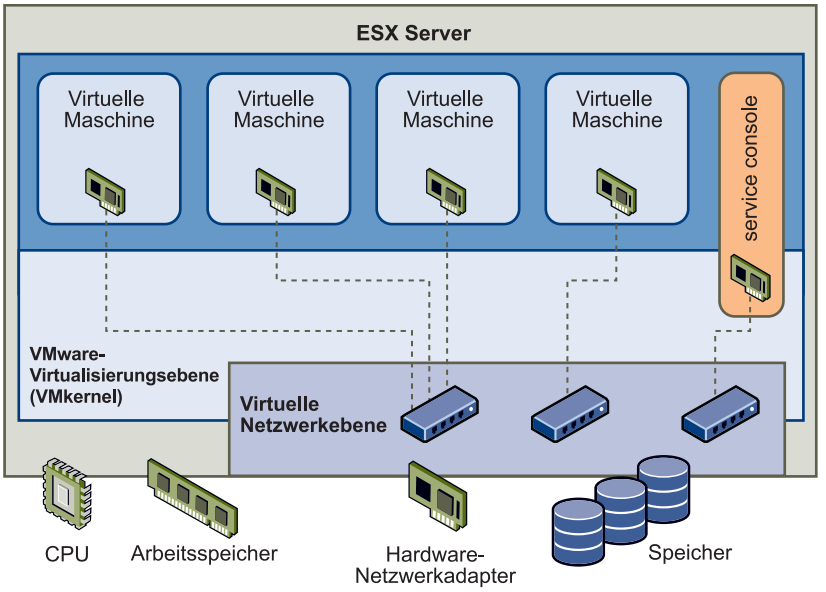
Dieses Kapitel umfasst die folgenden Abschnitte:

- „Architektur und Sicherheitsfunktionen von ESX Server 3“ auf Seite 173
- „Sonstige Quellen und Informationen zur Sicherheit“ auf Seite 186

Architektur und Sicherheitsfunktionen von ESX Server 3

Aus Sicht der Sicherheit besteht VMware ESX Server 3 aus vier Hauptkomponenten: der Virtualisierungsebene, den virtuellen Maschinen, der Servicekonsole und der virtuellen Netzwerkebene. Abbildung 9-1 bietet eine Übersicht über diese Komponenten.

Abbildung 9-1. ESX Server 3-Architektur



Jede dieser Komponenten und die gesamte Architektur wurden so entworfen, dass die Sicherheit des ESX Server 3-Systems als Ganzes gewährleistet wird.

Sicherheit und die Virtualisierungsebene

Die Virtualisierungsebene (bzw. VMkernel) ist ein Kernel, der von VMware für die Ausführung virtueller Maschinen entworfen wurde. Diese Ebene steuert die Hardware, die von den ESX Server-Hosts verwendet wird, und plant die Zuweisung von Hardwareressourcen an die einzelnen virtuellen Maschinen. Da VMkernel ausschließlich zur Unterstützung virtueller Maschinen verwendet wird, beschränkt sich die Schnittstelle zu VMkernel auf die API, die zur Verwaltung der virtuellen Maschinen notwendig ist.

Sicherheit und virtuelle Maschinen

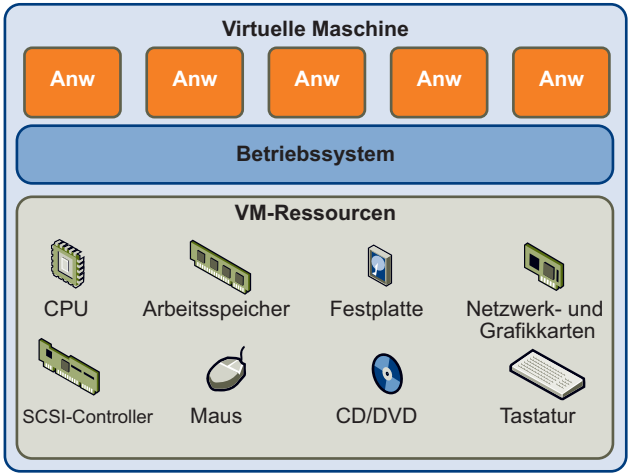
Virtuelle Maschinen sind die „Container“, in denen Anwendungen und Gastbetriebssysteme ausgeführt werden. Alle virtuellen Maschinen von VMware sind voneinander isoliert. Virtuelle Maschinen sind so konzipiert, dass sie alle Benutzer innerhalb des Gastbetriebssystems ungeachtet von deren Berechtigungen enthalten. Sogar Administratoren sind von anderen virtuellen Maschinen auf dieselbe Weise isoliert wie von anderen phyischen Computern.

Durch diese Isolierung können mehrere virtuelle Maschinen gleichzeitig und sicher auf der gleichen Hardware ausgeführt werden. Dabei werden sowohl Hardwarezugriff als auch ununterbrochene Leistung garantiert. Wenn zum Beispiel ein Gastbetriebssystem in einer virtuellen Maschine abstürzt, werden die anderen virtuellen Maschinen auf dem gleichen ESX Server-Host weiter ohne Beeinträchtigung ausgeführt. Der Absturz des Gastbetriebssystems hat keinen Einfluss auf Folgendes:

- Den uneingeschränkten Zugriff der Benutzer auf die anderen virtuellen Maschinen
- Den uneingeschränkten Zugriff der anderen virtuellen Maschinen auf die Ressourcen, die sie benötigen
- Die Leistung der anderen virtuellen Maschinen

Jede virtuelle Maschine ist von den anderen virtuellen Maschinen, die auf der gleichen Hardware ausgeführt werden, isoliert. Obwohl sich die virtuellen Maschinen die physischen Ressourcen wie CPU, Arbeitsspeicher und E/A-Geräte teilen, kann das Gastbetriebssystem einer einzelnen virtuellen Maschine nur die virtuellen Geräte sehen, die ihm zur Verfügung gestellt wurden (siehe Abbildung 9-2).

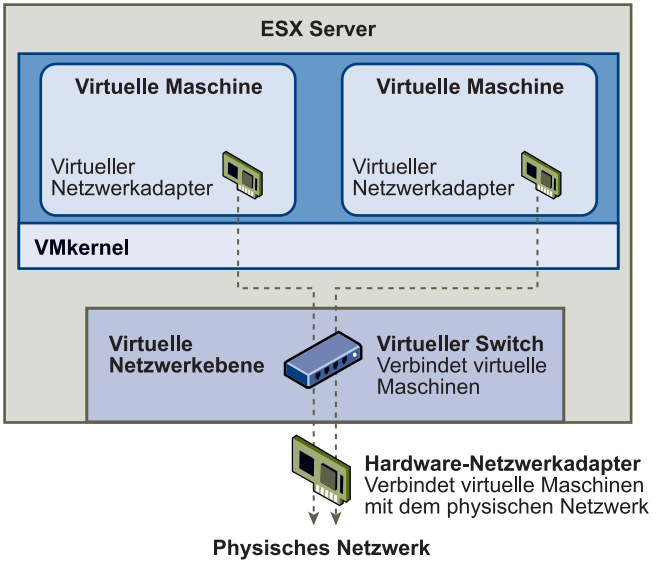
Abbildung 9-2. Isolierung virtueller Maschinen



Da VMkernel die physischen Ressourcen vermittelt und jeder Zugriff auf die physische Hardware über VMkernel erfolgt, können die virtuellen Maschinen diese Isolierungsebene nicht umgehen.

So wie ein Computer mit anderen Computern in einem Netzwerk nur über eine Netzwerkkarte kommunizieren kann, kann eine virtuelle Maschine mit anderen virtuellen Maschinen auf dem gleichen ESX Server-Host nur über einen virtuellen Switch kommunizieren. Außerdem kann die virtuelle Maschine mit einem physischen Netzwerk (einschließlich virtueller Maschinen auf anderen ESX Server-Hosts) nur über einen physischen Netzwerkadapter kommunizieren (siehe Abbildung 9-3).

Abbildung 9-3. Virtuelle Netzwerkanbindung über virtuelle Switches



Für die Isolierung virtueller Maschinen im Netzwerk gelten folgende Regeln:

- Wenn sich eine virtuelle Maschine keinen virtuellen Switch mit anderen virtuellen Maschinen teilt, ist sie von den virtuellen Netzwerken auf dem Host vollständig getrennt.
- Wenn einer virtuellen Maschine kein physischer Netzwerkadapter zugewiesen wurde, ist die virtuelle Maschine vollständig von physischen Netzwerken getrennt.
- Wenn Sie zum Schutz einer virtuellen Maschine vor dem Netzwerk die gleichen Sicherheitsmaßnahmen wie für normale Computer verwenden (Firewalls, Antiviren-Software usw.), ist die virtuelle Maschine genau so sicher, wie es ein Computer wäre.

Sie können die virtuelle Maschine außerdem durch die Einrichtung von Ressourcenreservierungen und -einschränkungen auf dem ESX Server-Host schützen. So können Sie zum Beispiel eine virtuelle Maschine mit den detaillierten Werkzeugen zur Ressourcensteuerung, die Ihnen in ESX Server zur Verfügung stehen, so konfigurieren, dass sie immer mindestens zehn Prozent der CPU-Ressourcen des ESX Server-Hosts erhält, nie jedoch mehr als zwanzig Prozent.

Ressourcenreservierungen und -einschränkungen schützen die virtuellen Maschinen vor Leistungsabfällen, wenn eine andere virtuelle Maschine versucht, zu viele Ressourcen der gemeinsam genutzten Hardware zu verwenden. Wenn zum Beispiel eine virtuelle Maschine auf dem ESX Server-Host durch eine Denial-Of-Service (DoS)- oder Distributed Denial-of-Service (DDoS)-Angriff außer Gefecht gesetzt wird, verhindert eine Einschränkung, dass der Angriff so viele Hardware-Ressourcen einnimmt, dass die anderen virtuellen Maschinen ebenfalls betroffen werden. Ebenso stellt eine Ressourcenreservierung für jede virtuelle Maschine sicher, dass bei hohen Ressourcenanforderungen durch den DoS-Angriff alle anderen virtuellen Maschinen immer noch über genügend Kapazitäten verfügen.

Standardmäßig schreibt der ESX Server eine Art der Ressourcenreservierung vor, indem er einen Verteilungsalgorithmus verwendet, der die verfügbaren Hostressourcen zu gleichen Teilen auf die virtuellen Maschinen verteilt und gleichzeitig einen bestimmten Prozentsatz der Ressourcen für einen Einsatz durch andere Systemkomponenten, wie z. B. die Servicekonsole bereithält. Dieses Standardverhalten bietet einen natürlichen Schutz gegen DoS- und DDoS-Angriffe. Geben Sie die spezifischen Ressourcenreservierungen und Grenzwerte individuell ein, wenn Sie das Standardverhalten auf Ihre Bedürfnisse so zuschneiden wollen, dass die Verteilung über die gesamte Konfiguration der virtuellen Maschine nicht einheitlich ist. Eine Erläuterung der Verwaltung der Ressourcenzuweisung für virtuelle Maschinen finden Sie im *Handbuch zur Ressourcenverwaltung*.

Sicherheit und die Servicekonsole

Die Servicekonsole von ESX Server 3 ist eine eingeschränkte Linux-Version, die auf Red Hat Enterprise Linux 3, Aktualisierung 8 (RHEL 3 U8) beruht. Die Servicekonsole stellt eine Ausführungsumgebung für die Überwachung und Verwaltung des gesamten ESX Server 3-Hosts zur Verfügung.

Wenn die Servicekonsole auf bestimmte Weise beeinträchtigt wird, ist auch die von ihr gesteuerte virtuelle Maschine gefährdet. Um das Risiko eines Angriffs über die Servicekonsole zu minimieren, wird die Servicekonsole von VMware durch eine Firewall geschützt. Weitere Informationen zu dieser Firewall finden Sie unter „Konfiguration der Servicekonsolen-Firewall“ auf Seite 249.

Neben der Implementierung der Firewall der Servicekonsole verringert VMware die Risiken für die Servicekonsole auf folgende Weise:

- ESX Server 3 führt nur Dienste aus, die zur Verwaltung seiner Funktionen unabdingbar sind. Die Servicekonsole beschränkt sich auf die Funktionen, die zum Betrieb von ESX Server 3 notwendig sind.
- Die Standardeinstellung für die Sicherheit von ESX Server 3 wird bei der Installation auf „hoch“ gesetzt, d. h. alle nach außen gerichteten Ports werden geschlossen und die wenigen freigegebenen, nach innen gerichteten Ports sind die Ports, die für die Kommunikation mit Clients wie dem VMware Virtual Infrastructure-Client notwendig sind. VMware empfiehlt die Beibehaltung dieser Sicherheitseinstellung, wenn die Servicekonsole nicht an ein vertrauenswürdiges Netzwerk angeschlossen ist.
- Standardmäßig sind alle Ports, die nicht spezifisch für den Verwaltungszugriff auf die Servicekonsole notwendig sind, geschlossen. Wenn Sie zusätzliche Dienste benötigen, müssen Sie die jeweiligen Ports öffnen.
- Standardmäßig wird der gesamte Datenverkehr zwischen Clients per SSL verschlüsselt. Die SSL-Verbindung verwendet eine 256-Bit-AES-Blockverschlüsselung und 1024-Bit-RSA-Schlüsselverschlüsselung.
- Der Webdienst Tomcat, der intern von ESX Server 3 zum Zugriff auf die Servicekonsole über Webclients wie Virtual Infrastructure Web Access verwendet wird, wurde so angepasst, dass er nur die für die Verwaltung und Überwachung über einen Webclient notwendigen Funktionen ausführt. Daher ist ESX Server 3 nicht von den Sicherheitslücken betroffen, die für Tomcat in weiter gefassten Anwendungsbereichen gemeldet wurden.
- VMware überwacht alle Sicherheitswarnungen, die die Sicherheit der Servicekonsole beeinflussen können, und veröffentlicht ggf. Sicherheitspatches. Gleiches gilt auch für andere Sicherheitslücken, die ESX Server 3-Hosts gefährden könnten. VMware veröffentlicht Sicherheitspatches für RHEL 3 U6 und höher, sobald sie zur Verfügung stehen.
- Unsichere Dienste, wie z. B. FTP und Telnet sind nicht installiert, und die Ports für diese Dienste sind standardmäßig geschlossen. Da sicherere Dienste wie SSH und SFTP leicht verfügbar sind, sollten Sie stets auf einen Einsatz der unsicheren Dienste zugunsten der sichereren Alternativen verzichten. Wenn Sie die unsicheren Dienste verwenden müssen und für die Servicekonsole einen ausreichenden Schutz hergestellt haben, müssen Sie entsprechend deren Ports öffnen, um sie zu unterstützen.

- Die Zahl der Anwendungen, die die Kennzeichen `setuid` oder `setgid` verwenden, wurde minimiert. Sie können alle `setuid`- oder `setgid`-Anwendungen deaktivieren, die für den Betrieb von ESX 3 Server optional sind. Weitere Informationen zu notwendigen und optionalen `setuid`- und `setgid`-Anwendungen finden Sie unter „setuid- und setgid-Anwendungen“ auf Seite 263.

Genauere Erläuterungen zu diesen Sicherheitsmaßnahmen und anderen Sicherheitsempfehlungen für die Servicekonsole finden Sie unter „Sicherheit der Servicekonsole“ auf Seite 247.

Sie können zwar bestimmte Programme, die für RHEL 3 U6 entwickelt wurden, in der Servicekonsole installieren und ausführen, dies kann jedoch zu ernsthaften Sicherheitslücken führen und wird daher nur unterstützt, wenn VMware dies ausdrücklich anführt. Wenn eine Sicherheitslücke in der unterstützten Konfiguration erkannt wird, informiert VMware alle Kunden mit geltenden Support- und Wartungsverträgen und stellt alle notwendigen Patches zur Verfügung.

HINWEIS Bestimmte Sicherheitsmeldungen von Red Hat betreffen die ESX Server 3-Umgebung nicht. In diesem Fall veröffentlicht VMware keine Warnungen oder Patches.

Weitere Informationen zu den VMware-Richtlinien für Sicherheitspatches unterstützter Programme sowie die Richtlinien für nicht unterstützte Software finden Sie unter „Sonstige Quellen und Informationen zur Sicherheit“ auf Seite 186.

Sicherheit und die virtuelle Netzwerkebene

Die virtuelle Netzwerkebene besteht aus den virtuellen Netzwerkgeräten, über die die virtuellen Maschinen und die Schnittstelle der Servicekonsole mit dem Rest des Netzwerks kommunizieren. ESX Server verwendet zur Kommunikation zwischen den virtuellen Maschinen und ihren Benutzern die virtuelle Netzwerkebene. Außerdem verwenden ESX Server-Hosts die virtuelle Netzwerkebene zur Kommunikation mit iSCSI-SANs, NAS-Speicher usw. Zur virtuellen Netzwerkebene gehören virtuelle Netzwerkadapter und virtuelle Switches.

Die Methoden, die Sie zur Absicherung eines Netzwerks von virtuellen Maschinen verwenden, hängen unter anderem davon ab, welches Gastbetriebssystem installiert wurde und ob die virtuellen Maschinen in einer sicheren Umgebung betrieben werden. Virtuelle Switches bieten einen hohen Grad an Sicherheit, wenn sie in Verbindung mit anderen üblichen Sicherheitsmaßnahmen, z. B. Firewalls, verwendet werden. ESX Server unterstützt auch VLANs nach IEEE 802.1q, die zum weiteren Schutz des Netzwerks der virtuellen Maschinen, der Servicekonsole oder der Speicherkonfiguration verwendet werden können. Mit VLANs können Sie ein physisches Netzwerk in Segmente aufteilen, sodass zwei Computer im gleichen physischen Netzwerk nur dann Pakete untereinander versenden können, wenn sie sich im gleichen VLAN befinden.

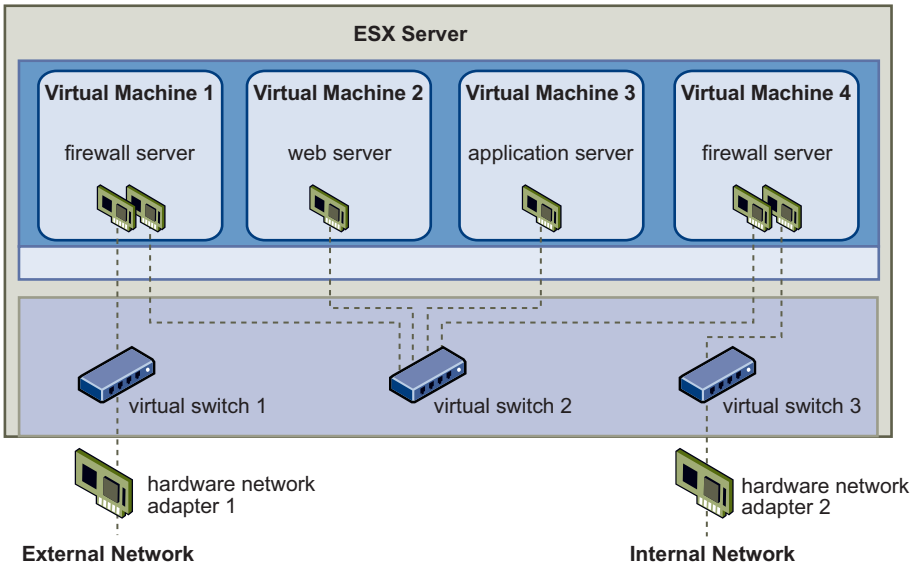
In den folgenden Beispielen wird ein Eindruck vermittelt, wie Sie virtuelle Switches dazu verwenden können, um Sicherheitsmaßnahmen wie DMZs zu implementieren und virtuelle Maschinen in verschiedenen Netzwerken auf dem gleichen ESX Server-Host zu konfigurieren.

HINWEIS Eine eingehende Abhandlung darüber, wie virtuelle Switches und VLANs zum Schutz des Netzwerks der virtuellen Maschinen beitragen können, sowie Sicherheitsempfehlungen für Netzwerke virtueller Maschinen finden Sie unter „Absichern virtueller Maschinen durch VLANs“ auf Seite 203.

Beispiel: Erstellen einer Netzwerk-DMZ auf einem einzelnen ESX Server-Host

Ein Beispiel für die Anwendung der ESX Server-Isolierung und virtueller Netzwerkfunktionen zur Umgebungsabsicherung ist die Einrichtung einer so genannten „demilitarisierten Zone (DMZ)“ auf einem einzelnen ESX Server-Host (siehe Abbildung 9-4).

Abbildung 9-4. Konfigurierte DMZ auf einem einzelnen ESX Server-Host



Diese Konfiguration umfasst vier virtuelle Maschinen, die so konfiguriert wurden, dass sie eine virtuelle DMZ auf dem virtuellen Switch 2 bilden. Die virtuelle Maschine 1 und die virtuelle Maschine 4 führen Firewalls aus und sind über virtuelle Switches an virtuelle Adapter angeschlossen. Diese beiden virtuellen Maschinen sind mehrfach vernetzt. Auf der virtuellen Maschine 2 wird ein Web-Server, auf der virtuellen Maschine 3 ein Anwendungs-Server ausgeführt. Diese beiden Maschinen sind einfach vernetzt.

Der Webserver und der Anwendungsserver befinden sich in der DMZ zwischen den zwei Firewalls. Die Verbindung zwischen diesen Elementen ist der virtuelle Switch 2, der die Firewalls mit den Servern verbindet. Dieser Switch ist nicht direkt mit Elementen außerhalb der DMZ verbunden und wird durch die beiden Firewalls vom externen Datenverkehr abgeschirmt.

Während des Betriebs der DMZ betritt externer Datenverkehr aus dem Internet die virtuelle Maschine 1 über den Hardware-Netzwerkadapter 1 (weitergeleitet vom virtuellen Switch 1) und wird von der auf dieser virtuellen Maschine installierten Firewall überprüft. Wenn die Firewall den Datenverkehr autorisiert, wird er an den virtuellen Switch in der DMZ, den virtuellen Switch 2, weitergeleitet. Da der Webserver und der Anwendungsserver ebenfalls an diesen Switch angeschlossen sind, können sie die externen Anforderungen bearbeiten.

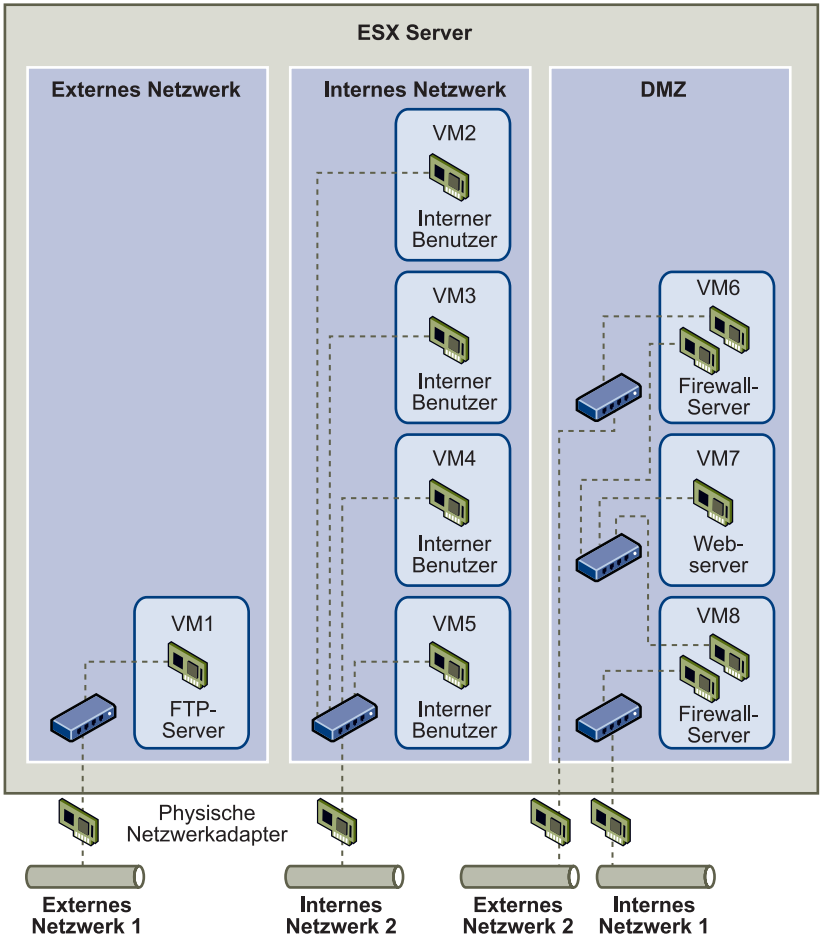
Der virtuelle Switch 2 ist auch an die virtuelle Maschine 4 angeschlossen. Auf dieser virtuellen Maschine schirmt eine Firewall die DMZ vom internen Firmennetzwerk ab. Diese Firewall filtert Pakete vom Web- und Anwendungsserver. Wenn ein Paket überprüft wurde, wird es über den virtuellen Switch 3 an den Hardware-Netzwerkadapter 2 weitergeleitet. Der Hardware-Netzwerkadapter 2 ist an das interne Firmennetzwerk angeschlossen.

Bei der Implementierung einer DMZ auf einem einzelnen ESX Server können Sie relativ einfache Firewalls verwenden. Obwohl eine virtuelle Maschine in dieser Konfiguration keine direkte Kontrolle über eine andere virtuelle Maschine ausüben oder auf ihren Speicher zugreifen kann, sind die virtuellen Maschinen dennoch über ein virtuelles Netzwerk verbunden. Dieses Netzwerk kann für die Verbreitung von Viren oder für andere Angriffe missbraucht werden. Die virtuellen Maschinen in der DMZ sind ebenso sicher wie getrennte physische Computer, die an dasselbe Netzwerk angeschlossen sind.

Beispiel: Erstellen mehrerer Netzwerke auf einem einzelnen ESX Server-Host

Das ESX Server-System wurde so entworfen, dass Sie bestimmte Gruppen virtueller Maschinen an das interne Netzwerk anbinden können, andere an das externe Netzwerk, und wiederum andere an beide Netzwerke, und zwar alles auf demselben ESX Server-Host. Diese Fähigkeit basiert auf der grundlegenden Isolierung virtueller Maschinen im Zusammenspiel mit der überlegt geplanten Nutzung von Funktionen zur virtuellen Vernetzung (siehe Abbildung 9-5).

Abbildung 9-5. Konfigurierte externe Netzwerke, interne Netzwerke und DMZ auf einem ESX Server-Host



Hier wurde ein ESX Server-Host vom Systemadministrator in drei eigenständige virtuelle Maschinenzonen eingeteilt, von denen jede eine bestimmte Funktion erfüllt:

- **FTP-Server** – Virtuelle Maschine 1 wurde mit FTP-Software konfiguriert und fungiert als Speicherbereich für Daten zu und von externen Ressourcen, wie z. B. von einem Sprachdienstleister lokalisierte Formulare und Begleitmaterialien.

  Diese virtuelle Maschine ist nur mit dem externen Netzwerk verbunden. Sie verfügt über einen eigenen virtuellen Switch und physischen Netzwerkadapter, die sie mit dem externen Netzwerk 1 verbinden. Dieses Netzwerk ist auf Server beschränkt, die vom Unternehmen zum Empfang von Daten aus externen Quellen verwendet werden. Das Unternehmen verwendet beispielsweise das externe Netzwerk 1, um FTP-Daten von Dienstleistern zu empfangen und den Dienstleistern FTP-Zugriff auf Daten zu gewähren, die auf extern verfügbaren Servern gespeichert sind. Zusätzlich zur Verarbeitung der Daten für die virtuelle Maschine 1 verarbeitet das externe Netzwerk 1 auch Daten für FTP-Server auf anderen ESX Server-Hosts am Standort.

  Da sich die virtuelle Maschine 1 keinen virtuellen Switch oder physischen Netzwerkadapter mit anderen virtuellen Maschinen auf dem Host teilt, können die anderen virtuellen Maschinen auf dem Host keine Datenpakete in das Netzwerk der virtuellen Maschine 1 übertragen oder daraus empfangen. Dadurch werden Spionageangriffe verhindert, da dem Opfer dafür Netzwerkdaten gesendet werden müssen. Außerdem kann der Angreifer dadurch die natürliche Anfälligkeit von FTP nicht zum Zugriff auf andere virtuelle Maschinen auf dem Host nutzen.

- Die **internen virtuellen Maschinen** – die virtuellen Maschinen 2 bis 5, sind der internen Verwendung vorbehalten. Diese virtuellen Maschinen verarbeiten und speichern vertrauliche firmeninterne Daten wie medizinische Unterlagen, juristische Dokumente und Betrugsermittlungen. Daher müssen Systemadministratoren für diese virtuellen Maschinen den höchsten Schutz gewährleisten.

  Diese virtuellen Maschinen sind über ihren eigenen virtuellen Switch und physischen Netzwerkadapter an das interne Netzwerk 2 angeschlossen. Das Interne Netzwerk 2 ist der internen Nutzung durch Mitarbeiter wie Reklamationssachbearbeiter, firmeninterne Anwälte und andere Sachbearbeiter vorbehalten.

Die virtuellen Maschinen 2 bis 5 können über den virtuellen Switch untereinander und über den physischen Netzwerkadapter mit internen Maschinen an anderen Stellen des internen Netzwerks 2 kommunizieren. Sie können nicht mit Computern oder virtuellen Maschinen kommunizieren, die Zugang zu den externen Netzwerken haben. Wie beim FTP-Server können diese virtuellen Maschinen keine Datenpakete an Netzwerke anderer virtueller Maschinen senden oder sie von diesen empfangen. Ebenso können die anderen virtuellen Maschinen keine Datenpakete an die virtuellen Maschinen 2 bis 5 senden oder von diesen empfangen.

- **DMZ** – Die virtuellen Maschinen 6 bis 8 wurden als DMZ konfiguriert, die von der Marketingabteilung dazu verwendet wird, die externe Webseite des Unternehmens bereitzustellen.

  Diese Gruppe virtueller Maschinen ist dem externen Netzwerk 2 und dem internen Netzwerk 1 zugeordnet. Das Unternehmen nutzt das externe Netzwerk 2 zur Unterstützung der Webserver, die von der Marketing- und der Finanzabteilung zur Bereitstellung der Unternehmenswebseite und anderer webbasierter Anwendungen für externe Nutzer verwendet werden. Das interne Netzwerk 1 ist der Verbindungskanal, den die Marketingabteilung zur Veröffentlichung von Webseiten auf der Unternehmenswebseite, zur Bereitstellung von Downloads und Diensten wie Benutzerforen verwendet.

  Da diese Netzwerke vom externen Netzwerk 1 und internen Netzwerk 2 getrennt sind und die virtuellen Maschinen keine gemeinsamen Kontaktpunkte (Switches oder Adapter) aufweisen, besteht kein Angriffsrisiko für den FTP-Server oder die Gruppe interner virtueller Maschinen (weder als Ausgangspunkt noch als Ziel).

  Ein Beispiel für die Konfiguration einer DMZ unter Verwendung virtueller Maschinen finden Sie unter „Beispiel: Erstellen einer Netzwerk-DMZ auf einem einzelnen ESX Server-Host“ auf Seite 180.

Wenn die Isolierung der virtuellen Maschinen genau beachtet wird, die virtuellen Switches ordnungsgemäß konfiguriert werden und die Netzwerktrennung eingehalten wird, können alle drei Zonen virtueller Maschinen auf dem gleichen ESX Server-Host untergebracht werden, ohne dass Datenverluste oder Ressourcenmissbräuche befürchtet werden müssen.

Das Unternehmen erzwingt die Isolierung der virtuellen Maschinengruppen durch die Verwendung mehrerer interner und externer Netzwerke und die Sicherstellung, dass die virtuellen Switches und physischen Netzwerkadapter jeder Gruppe von denen anderer Gruppen vollständig getrennt sind.

Da keiner der virtuellen Switches sich über mehrere Zonen erstreckt, wird das Risiko des Durchsickerns von Daten von einer Zone in eine andere ausgeschaltet. Ein virtueller Switch kann aufbaubedingt keine Datenpakete direkt an einen anderen virtuellen Switch weitergeben. Datenpakete können nur unter folgenden Umständen von einem virtuellen Switch zu einem anderen gelangen:

- Wenn die virtuellen Switches an das gleiche physische LAN angeschlossen sind
- Wenn die virtuellen Switches an eine gemeinsame virtuelle Maschine angeschlossen sind, die dann dazu verwendet werden kann, Datenpakete zu übertragen

In der Beispielkonfiguration wird keine dieser Bedingungen erfüllt. Wenn der Systemadministrator prüfen möchten, ob es einen gemeinsamen virtuellen Switch-Pfad gibt, kann dies über die Überprüfung möglicher gemeinsamer Kontaktpunkte im Netzwerkswitchplan im VI-Client oder über VI Web Access geschehen. Weitere Informationen zur Übersicht über die virtuellen Switches finden Sie unter „Virtuelle Switches“ auf Seite 22.

Zum Schutz der Hardwareressourcen der virtuellen Maschinen kann der Systemadministrator eine Reservierung und Einschränkung der Ressourcen für jede virtuelle Maschine vornehmen, um das Risiko von DoS- und DDoS-Angriffen einzudämmen. Der Systemadministrator kann den ESX Server-Host und die virtuellen Maschinen außerdem durch die Installation von Softwarefirewalls im Front-End und Back-End der DMZ, durch Positionierung des ESX Server-Hosts hinter einer physischen Firewall und durch Anschluss der Servicekonsole und der an das Netzwerk angeschlossenen Speicherressourcen an jeweils einen eigenen virtuellen Switch schützen.

Sonstige Quellen und Informationen zur Sicherheit

In folgenden Quellen finden Sie zusätzliche Informationen zu Sicherheitsthemen.

Tabelle 9-1. Sicherheitsressourcen von VMware im Internet

Thema	Ressource
Sicherheitsrichtlinien von VMware, aktuelle Sicherheitswarnungen, Sicherheitsdownloads und themenspezifische Abhandlungen zu Sicherheitslücken	www.vmware.com/security/ communities.vmware.com/community/vmtn/general/security
Richtlinie zur Sicherheitsantwort	http://www.vmware.com/support/policies/security_response.html VMware hat es sich zur Aufgabe gemacht, Sie bei der Absicherung Ihrer virtuellen Umgebung zu unterstützen. Damit Sie sicher sein können, dass alle Sicherheitslücken so schnell wie möglich eliminiert werden, haben wir die VMware-Richtlinie zur Sicherheitsantwort verfasst, um unseren Einsatz für dieses Ziel zu dokumentieren.
Unterstützung von Drittanbieter-Software	http://www.vmware.com/support/policies VMware unterstützt viele Speichersysteme und Software-Agenten wie Sicherungs-Agenten, Systemverwaltungs-Agenten usw. Ein Verzeichnis der von ESX Server 3 unterstützten Agenten, Werkzeuge und anderer Software finden Sie über das Durchsuchen der ESX Server 3-Kompatibilitätshandbücher unter http://www.vmware.com/vmtn/resources. Die Branche bietet mehr Produkte und Konfigurationen an, als VMware testen kann. Wenn VMware ein Produkt oder eine Konfiguration nicht in einem Kompatibilitätshandbuch nennt, wird der technische Support versuchen, Ihnen bei Problemen zu helfen, kann jedoch nicht garantieren, dass das Produkt oder die Konfiguration verwendet werden kann. Testen Sie die Sicherheitsrisiken für nicht unterstützte Produkte oder Konfigurationen immer sorgfältig.

Absichern einer ESX Server 3-Konfiguration 10

In diesem Kapitel werden die Maßnahmen beschrieben, mit denen Sie die Umgebung für Ihre ESX Server 3-Hosts, virtuellen Maschinen und iSCSI-SANs absichern können. Diese Abhandlung konzentriert sich auf den sicherheitsbezogenen Netzwerkkonfigurationsaufbau und die Maßnahmen, mit denen Sie die Komponenten in Ihrer Konfiguration vor Angriffen schützen können.

In diesem Kapitel werden folgende Themen behandelt:

- „Absichern des Netzwerks mit Firewalls“ auf Seite 187
- „Absichern virtueller Maschinen durch VLANs“ auf Seite 203
- „Absichern von iSCSI-Speicher“ auf Seite 214

Absichern des Netzwerks mit Firewalls

Sicherheitsadministratoren verwenden Firewalls, um das Netzwerk oder ausgewählte Komponenten innerhalb des Netzwerks vor unerlaubten Zugriffen zu schützen. Firewalls kontrollieren den Zugriff auf die Geräte in ihrem Umfeld, indem sie alle Kommunikationspfade außer denen, die der Administrator explizit oder implizit als zulässig definiert, abriegeln. Dadurch wird die unerlaubte Verwendung der Geräte verhindert. Diese Pfade, die der Administrator in der Firewall öffnet, werden Ports genannt und lassen Datenverkehr zwischen Geräten auf den beiden Seiten der Firewall passieren.

In der virtuellen Maschinenumgebung können Firewalls in folgenden Varianten auftreten:

- Physische Maschinen, z. B. VirtualCenter Management Server- und ESX Server 3-Hosts.
- Zwischen zwei virtuellen Maschinen - beispielsweise zwischen einer virtuellen Maschine, die als externer Webserver dient, und einer virtuellen Maschine, die an das interne Firmennetzwerk angeschlossen ist.
- Zwischen einem physischen Computer und einer virtuellen Maschine, wenn Sie eine Firewall zwischen einen physischen Netzwerkadapter und eine virtuelle Maschine schalten.

Die Nutzung von Firewalls in einer ESX Server 3-Konfiguration hängt davon ab, wie Sie das Netzwerk nutzen möchten und wie sicher die einzelnen Komponenten sein müssen. Wenn Sie zum Beispiel ein virtuelles Netzwerk erstellen, in dem jede virtuelle Maschine eine andere Benchmark-Testsuite für die gleiche Abteilung ausführt, ist das Risiko ungewollten Zugriffs von einer virtuellen Maschine auf eine andere minimal. Deshalb ist es für diese Konfiguration in der Regel nicht erforderlich, Firewalls zwischen den virtuellen Maschinen einzurichten. Um jedoch eine Störung der Testläufe durch einen externen Host zu verhindern, kann die Konfiguration so eingerichtet werden, dass sich eine Firewall am Eingang zum virtuellen Netzwerk befindet, um alle virtuellen Maschinen zu schützen.

Dieser Abschnitt demonstriert die Einrichtung von Firewalls für Konfigurationen mit und ohne VirtualCenter. Hier finden Sie auch Informationen zu den Firewallports, die für ESX Server 3-Systeme notwendig sind.

- „Firewalls in Konfigurationen mit einem VirtualCenter Server“ auf Seite 189
- „Firewalls für Konfigurationen ohne VirtualCenter Server“ auf Seite 191
- „TCP- und UDP-Ports für den Verwaltungszugriff“ auf Seite 193
- „Herstellen einer Verbindung mit einem VirtualCenter Server über eine Firewall“ auf Seite 195
- „Herstellen einer Verbindung mit der VM-Konsole über eine Firewall“ auf Seite 196
- „Verbinden von ESX Server 3-Hosts über Firewalls“ auf Seite 198
- „Öffnen von Firewallports für unterstützte Dienste und Verwaltungs-Agenten“ auf Seite 198

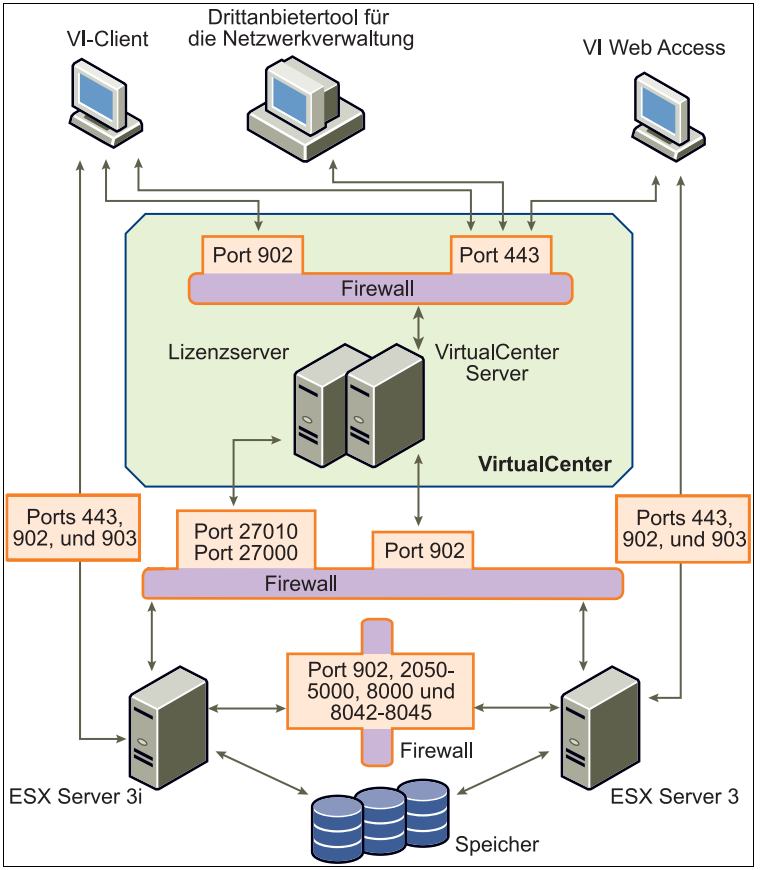
Informationen zur Firewall der Servicekonsole finden Sie unter „Konfiguration der Servicekonsolen-Firewall“ auf Seite 249. Informationen zu Konfiguration und Porteinstellungen während der Installation finden Sie im *Einrichtungshandbuch*.

Firewalls in Konfigurationen mit einem VirtualCenter Server

Wenn Sie einen VirtualCenter Server verwenden, können Sie Firewalls an allen in Abbildung 10-1 gezeigten Punkten installieren.

HINWEIS Abhängig von der Konfiguration sind ggf. nicht alle in der Abbildung dargestellten Firewalls notwendig, oder es sind zusätzliche, nicht dargestellte Firewalls nötig.

Abbildung 10-1. Beispiel für eine Virtual Infrastructure-Netzwerkkonfiguration und den Datenfluss



Netzwerke, die über einen VirtualCenter Server konfiguriert werden, können Daten über verschiedene Typen von Clients erhalten: den VI-Client, VI Web Access und Netzwerkverwaltungs-Clients von Drittanbietern, die über das SDK eine Schnittstelle zum Host einrichten. Während des normalen Betriebs wartet VirtualCenter an bestimmten Ports auf Daten von verwalteten Hosts und Clients. VirtualCenter geht auch davon aus, dass die verwalteten Hosts an bestimmten Ports auf Daten von VirtualCenter warten. Wenn sich zwischen diesen Elementen eine Firewall befindet, muss sichergestellt werden, dass Firewall-Ports für den Datenverkehr geöffnet wurden.

Wenn Sie über einen VirtualCenter Server auf ESX Server-Hosts zugreifen, wird der VirtualCenter Server normalerweise durch eine Firewall geschützt. Diese Firewall bietet einen Grundschutz für das Netzwerk. Ob sich die Firewall zwischen den Clients und dem VirtualCenter Server befindet oder sowohl der VirtualCenter Server als auch die Clients hinter einer gemeinsamen Firewall liegen, hängt vom Netzwerkaufbau ab. Wichtig ist es sicherzustellen, dass eine Firewall an den Punkten installiert wird, die Sie als Eingangspunkte in das ganze System betrachten.

Firewalls können auch an vielen anderen Zugriffspunkten im Netzwerk installiert werden. Dies hängt davon ab, wie das Netzwerk genutzt werden soll und wie sicher die verschiedenen Geräte sein müssen. Bestimmen Sie die Einsatzorte für Ihre Firewalls anhand der Sicherheitsrisiken, die eine Analyse der Netzwerkkonfiguration ergeben hat. Die folgende Liste führt verschiedene Einsatzorte für Firewalls auf, die in ESX Server 3-Implementierungen häufig auftreten. Viele der Einsatzorte für Firewalls in der Liste und Abbildung 10-1 sind optional.

- Zwischen dem Webbrowser und den HTTP- und HTTPS-Proxyservern für VI Web Access.
- Zwischen dem VI-Client, VI Web Access oder einem Netzwerkverwaltungs-Client von Drittanbietern und dem VirtualCenter Server.
- Wenn die Benutzer über den VI-Client auf virtuelle Maschinen zugreifen, zwischen dem VI-Client und dem ESX Server 3-Host. Diese Verbindung ist ein Zusatz zu der Verbindung zwischen dem VI-Client und dem VirtualCenter Server und benötigt einen anderen Port.
- Wenn die Benutzer über einen Webbrowser auf virtuelle Maschinen zugreifen, zwischen dem Webbrowser und dem ESX Server 3-Host. Diese Verbindung unterscheidet sich von der zwischen dem VI Web Access-Client und dem VirtualCenter Server und benötigt daher andere Ports.

- Zwischen dem Lizenzserver und entweder dem VirtualCenter Server oder dem ESX Server 3-Host. Normalerweise wird der Lizenzserver in Konfigurationen mit einem VirtualCenter Server auf dem gleichen Computer ausgeführt wie der VirtualCenter Server. In diesem Fall ist der Lizenzserver über eine Firewall an das ESX Server 3-Netzwerk angebunden - parallel zum VirtualCenter Server, nur über andere Ports.

  In einigen Konfigurationen wird ggf. ein externer Lizenz-Server verwendet, zum Beispiel wenn das Unternehmen alle Lizenzen über ein einzelnes für diesen Zweck reserviertes Gerät steuern möchte. In diesem Fall sollte der Lizenzserver über eine zwischengeschaltete Firewall an den VirtualCenter Server angebunden werden.

  Unabhängig von der Anbindung des Lizenzservers, sind die Ports, die für den Lizenzdatenverkehr verwendet werden, in jedem Fall gleich. Weitere Informationen zur Lizenzierung finden Sie im *Einrichtungshandbuch*.

- Zwischen dem VirtualCenter Server und den ESX Server 3-Hosts.

- Zwischen den ESX Server 3-Hosts im Netzwerk. Zwar ist der Datenverkehr zwischen den ESX Server 3-Hosts normalerweise vertrauenswürdig, Sie können jedoch bei befürchteten Sicherheitsrisiken zwischen den einzelnen Computern dennoch Firewalls zwischen den ESX Server 3-Hosts installieren.

  Wenn Sie Firewalls zwischen ESX Server 3-Hosts verwenden und virtuelle Maschinen auf einen anderen Server verschieben, klonen oder VMotion verwenden möchten, müssen auch Ports in allen Firewalls zwischen Quell- und Zielhost geöffnet werden, damit Quelle und Ziel miteinander kommunizieren können.

- Zwischen ESX Server 3-Hosts und Netzwerkspeicher, z. B. NFS- oder iSCSI-Speicher. Diese Ports sind nicht VMware-spezifisch und werden anhand der Spezifikationen für das jeweilige Netzwerk konfiguriert.

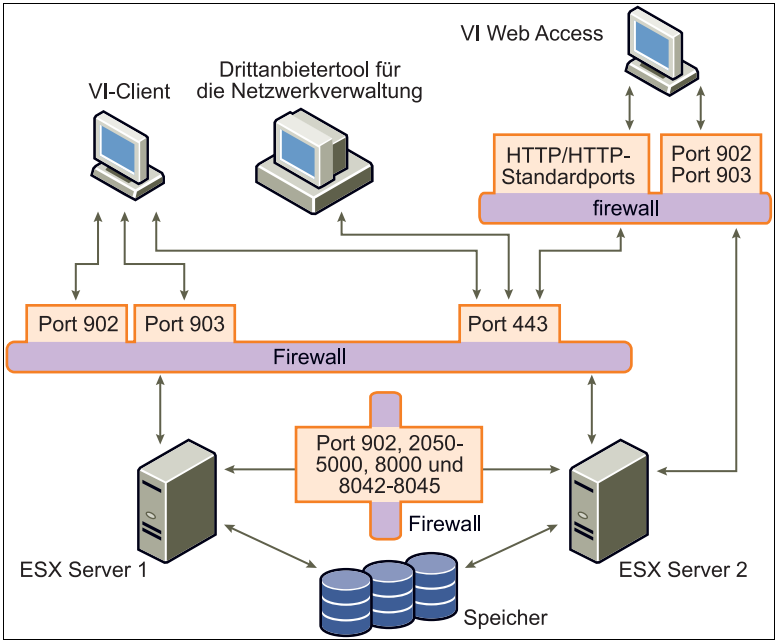
Informationen zu den Ports, die für diese Kommunikationspfade geöffnet werden müssen, finden Sie unter „TCP- und UDP-Ports für den Verwaltungszugriff“ auf Seite 193.

Firewalls für Konfigurationen ohne VirtualCenter Server

Wenn die Clients direkt, d. h. nicht über einen VirtualCenter Server, an das ESX Server 3-Netzwerk angebunden werden, gestaltet sich die Firewallkonfiguration etwas einfacher. Firewalls können an jeder der in Abbildung 10-2 gezeigten Stellen installiert werden.

HINWEIS Abhängig von der Konfiguration sind ggf. nicht alle in Abbildung 10-2 dargestellten Firewalls notwendig, oder es sind zusätzliche, nicht dargestellte Firewalls nötig.

Abbildung 10-2. Firewallkonfiguration für ESX Server 3-Netzwerke, die direkt über einen Client verwaltet werden



Netzwerke ohne VirtualCenter Server erhalten ihre Daten über die gleichen Typen von Clients wie Netzwerke mit einem VirtualCenter Server: VI Client, VI Web Access-Clients und Netzwerkverwaltungs-Clients von Drittanbietern. Größtenteils sind die Anforderungen der Firewall die gleichen, aber es gibt einige markante Unterschiede:

- Wie bei Konfigurationen mit einem VirtualCenter Server sollten Sie sicherstellen, dass die ESX Server -Ebene oder – je nach Konfiguration – die Clients und die ESX Server 3-Ebene geschützt sind. Diese Firewall bietet einen Grundschutz für das Netzwerk. Die verwendeten Firewallports sind die gleichen wie bei der Verwendung eines VirtualCenter Servers.
- Die Lizenzierung gehört in dieser Konfiguration zu dem ESX Server 3-Paket, das Sie auf allen ESX Server 3-Hosts installieren. Da die Lizenzierung über den Server abgewickelt wird, ist kein getrennter Lizenzserver notwendig. Dadurch entfällt die Firewall zwischen dem Lizenzserver und dem ESX Server 3-Netzwerk.

HINWEIS Unter bestimmten Umständen sollen Sie Lizenzen zentral verwaltet werden. Dazu können Sie einen getrennten Lizenzserver verwenden oder den Lizenzserver auf einem der ESX Server 3-Hosts im Netzwerk unterbringen. In beiden Fällen binden Sie den Lizenzserver wie beim Vorhandensein eines VirtualCenter Servers über eine Firewall an das ESX Server 3-Netzwerk an. Dazu werden die Ports verwendet, die normalerweise für die Lizenzierung virtueller Maschinen reserviert sind. Bei Konfigurationen, die einen anderen als den automatisch auf dem ESX Server 3-Host installierten Lizenzserver verwenden, ist eine zusätzliche Einrichtung notwendig. Weitere Informationen zur Lizenzierung finden Sie im *Einrichtungshandbuch*.

TCP- und UDP-Ports für den Verwaltungszugriff

In diesem Abschnitt werden voreingestellte TCP- und UDP-Ports behandelt, die für den Verwaltungszugriff auf den VirtualCenter Server, die ESX Server 3-Hosts und andere Netzwerkkomponenten verwendet werden. Wenn Netzwerkkomponenten, die außerhalb einer Firewall liegen, verwaltet werden müssen, muss ggf. die Firewall neu konfiguriert werden, damit auf die entsprechenden Ports zugegriffen werden kann.

HINWEIS Sofern nicht anders angegeben, sind die in Tabelle 10-1 aufgeführten Ports durch die Servicekonsolenschnittstelle angebunden.

Tabelle 10-1. TCP- und UDP-Ports

Port	Zweck	Art des Datenverkehrs
80	HTTP-Zugriff. Nicht abgesicherter, standardmäßiger TCP-Webport, der normalerweise in Verbindung mit Port 443 als Front-End für den Zugriff auf ESX Server -Netzwerke aus dem Internet verwendet wird. Port 80 leitet Datenverkehr auf eine HTTPS-Startseite (Port 443) um, von der Sie die Konsole der virtuellen Maschine aufrufen. Verwenden Sie Port 80 für Verbindungen zu VI-Web Access aus dem Internet. WS-Management verwendet Port 80.	Eingehendes TCP
427	Der CIM-Client verwendet das Service Location Protocol, Version 2 (SLPv2), zum Ermitteln von CIM-Servern.	Ein- und ausgehendes UDP

Tabelle 10-1. TCP- und UDP-Ports (Fortsetzung)

Port	Zweck	Art des Datenverkehrs
443	HTTPS-Zugriff Der Standard-SSL-Internetport. Verwenden Sie Port 443 für folgende Aufgaben: ■ Verbindung mit VI Web Access aus dem Internet. ■ Herstellen einer Verbindung zwischen VI Web Access und Netzwerkverwaltungs-Clients von Drittanbietern mit dem VirtualCenter Server ■ Direkter Zugriff von VI Web Access und Netzwerkverwaltungs-Clients von Drittanbietern auf ESX Server 3-Hosts ■ VI-Client-Zugriff auf den VirtualCenter Server ■ Direkter VI-Client-Zugriff auf die ESX Server 3-Hosts ■ WS-Verwaltung ■ VMware Update Manager ■ VMware Converter	Eingehendes TCP
902	Authentifizierungsdatenverkehr für ESX Server 3. Wählen Sie Port 902 für den ESX Server 3-Hostzugriff auf andere ESX Server 3-Hosts für Migrations- und Bereitstellungszwecke.	Eingehendes TCP, ausgehendes UDP
903	Datenverkehr der Remote-Steuerung, der durch Zugriffe der Benutzer auf virtuelle Maschinen auf einem bestimmten ESX Server 3-Host entsteht. Verwenden Sie Port 903 für folgende Aufgaben: ■ VI-Client-Zugriff auf die Konsolen virtueller Maschinen ■ VI Web Access Client-Zugriff auf die Konsolen virtueller Maschinen	Eingehendes TCP
2049	Datenübertragungen von den NFS-Speichergeräten. Dieser Port wird für die VMkernel-Schnittstelle, nicht für die Servicekonsolenschnittstelle verwendet.	Ein- und ausgehendes TCP
2050–2250	Datenverkehr zwischen ESX Server 3-Hosts für VMware High Availability (HA) und EMC Autostart Manager. Diese Ports werden von der VMKernel-Schnittstelle verwaltet.	Ausgehendes TCP, ein- und ausgehendes UDP
3260	Datenübertragungen von den iSCSI-Speichergeräten. Dieser Port wird für die VMkernel-Schnittstelle und die Servicekonsolenschnittstelle verwendet.	Ausgehendes TCP
5900-5906	RFB-Protokoll, das von Verwaltungstools wie VNC verwendet wird.	Ein- und ausgehendes TCP
5988	CIM-XML-Übertragungen über HTTPS.	Ein- und ausgehendes TCP

Tabelle 10-1. TCP- und UDP-Ports (Fortsetzung)

Port	Zweck	Art des Datenverkehrs
5989	CIM-XML-Übertragungen über HTTP.	Ein- und ausgehendes TCP
8000	Eingehende Anforderungen von VMotion. Dieser Port wird für die VMkernel-Schnittstelle, nicht für die Servicekonsolenschnittstelle verwendet.	Ein- und ausgehendes TCP
8042–8045	Datenverkehr zwischen ESX Server 3-Hosts für VMware HA und EMC Autostart Manager.	Ausgehendes TCP, ein- und ausgehendes UDP
27000	Lizenzübertragungen vom ESX Server 3-Host an den Lizenzserver (**lmgrd.exe**).	Ein- und ausgehendes TCP
27010	Lizenzübertragungen vom ESX Server 3-Host an den Lizenzserver (**vmwarelm.exe**).	Ein- und ausgehendes TCP

Zusätzlich zu den aufgeführten TCP- und UDP-Ports können Sie andere Ports je nach Ihren Bedürfnissen konfigurieren:

- Mit dem VI-Client können Sie Ports für installierte Verwaltungs-Agenten und unterstützte Dienste wie SSH, NFS usw. freigeben. Informationen zur Konfiguration anderer Ports für diese Dienste finden Sie unter „Öffnen von Firewallports für unterstützte Dienste und Verwaltungs-Agenten“ auf Seite 198.
- Für andere Dienste und Agenten, die für Ihr Netzwerk notwendig sind, können Sie in der Servicekonsole weitere Firewall-Ports öffnen, indem Sie Befehlszeilenskripts ausführen. Siehe „Konfiguration der Servicekonsolen-Firewall“ auf Seite 249.

Herstellen einer Verbindung mit einem VirtualCenter Server über eine Firewall

Der Standardport (siehe Tabelle 10-1), der von VirtualCenter Server zum Überwachen der von seinen Clients ausgehenden Datenübertragung verwendet wird, ist Port 443. Wenn zwischen dem VirtualCenter Server und seinen Clients eine Firewall vorhanden ist, müssen Sie eine Verbindung konfigurieren, über die der VirtualCenter Server Daten von seinen Clients empfangen kann.

Damit der VirtualCenter Server Daten von einem Client empfangen kann, öffnen Sie Port 443. Zusätzliche Informationen zur Konfiguration von Ports in einer Firewall erhalten Sie vom Firewalladministrator.

Wenn Sie den VI-Client verwenden und nicht Port 443 als Port für den Datenverkehr zwischen VI Client und VirtualCenter Server verwenden möchten, können Sie den Port

über die VirtualCenter-Einstellungen auf dem VI-Client ändern. Informationen zur Änderung dieser Einstellungen finden Sie in *Grundlagen der Systemverwaltung*.

Herstellen einer Verbindung mit der VM-Konsole über eine Firewall

Sowohl bei der Anbindung des Clients an die ESX Server 3-Hosts über einen VirtualCenter Server als auch bei der Verwendung einer direkten Verbindung mit dem ESX Server-Host sind bestimmte Hosts für die Kommunikation zwischen Administrator bzw. Benutzer und den Konsolen für virtuellen Maschinen notwendig. Diese Ports unterstützen verschiedene Clientfunktionen, verbinden unterschiedliche Ebenen innerhalb von ESX Server 3 und verwenden verschiedene Authentifizierungsprotokolle. Sie lauten wie folgt:

- **Port 902** – Der VirtualCenter Server verwendet diesen Port, um Daten an die von VirtualCenter verwalteten Hosts zu senden. Port 902 ist der Port, den der VirtualCenter Server für verfügbar hält, wenn Daten an den ESX Server 3-Host gesendet werden. VMware unterstützt keinen anderen Port für die Konfiguration dieser Verbindung.

  Port 902 verbindet den VirtualCenter Server mit ESX Server 3-Host über den VMware Authorization Daemon (`vmware-authd`). Dieser Daemon überträgt anschließend Daten an Port 902 zur Verarbeitung an die entsprechenden Empfänger.

- **Port 443** – Der VI-Client, der VI Web Access-Client und das SDK verwenden diesen Port, um Daten an die von VirtualCenter verwalteten Hosts zu senden. Der VI-Client, der VI Web Access-Client und das SDK verwenden diesen Port auch, wenn sie direkt mit dem ESX Server 3-Host verbunden sind, um Verwaltungsfunktionen für den Server und seine virtuellen Maschinen durchzuführen. Port 443 ist der Port, den die Clients für verfügbar halten, wenn Daten an den ESX Server 3-Host gesendet werden. VMware unterstützt für diese Verbindungen nur diesen Port.

  Port 443 verbindet Clients mit dem ESX Server 3-Host über den Webdienst Tomcat oder das SDK. `vmware-hostd` überträgt anschließend Daten an Port 443 zur Verarbeitung an die entsprechenden Empfänger.

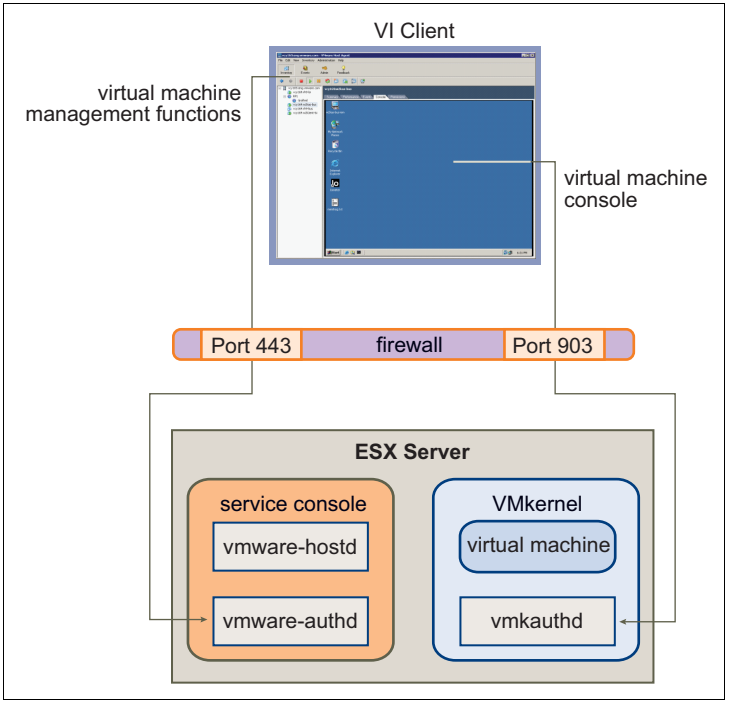
- **Port 903** – Der VI-Client und VI Web Access verwenden diesen Port für Verbindungen der Maus-/Tastatur-/Bildschirmaktivitäten des Gastbetriebssystems auf virtuellen Maschinen. Die Benutzer interagieren über diesen Port mit dem Gastbetriebssystem und den Anwendungen der virtuellen Maschine. Port 903 ist der Port, den der VI-Client und VI Web Access für verfügbar

halten, wenn sie mit virtuellen Maschinen kommunizieren. Für diese Aufgabe unterstützt VMware nur diesen Port.

Port 903 verbindet den VI-Client mit einer bestimmten virtuellen Maschine, die auf dem ESX Server 3-Host konfiguriert wurde.

Abbildung 10-3 zeigt die Beziehungen zwischen VI-Client-Funktionen, Ports und ESX Server 3-Prozessen. Der VI Web Access-Client verwendet für seine Kommunikation mit dem ESX Server 3-Host dieselbe Grundzuordnung.

Abbildung 10-3. Port-Verwendung für VI-Clientdatenverkehr mit ESX Server 3



Wenn Sie zwischen dem VirtualCenter Server und dem von VirtualCenter verwalteten Hosts eine Firewall installiert haben, müssen Sie die Ports 443 und 903 in der Firewall öffnen, um folgenden Datenverkehr zuzulassen:

- Vom VirtualCenter Server zu ESX Server 3-Hosts.
- Direkt vom VI-Client und von VI Web Access zu den ESX Server 3-Hosts.

Weitere Informationen zur Konfiguration der Ports erhalten Sie beim Firewalladministrator.

Verbinden von ESX Server 3-Hosts über Firewalls

Wenn Sie eine Firewall zwischen zwei ESX Server 3-Hosts eingerichtet haben und Datenübertragungen zwischen den Hosts ermöglichen oder mit VirtualCenter Quell/Ziel-Aktivitäten wie Datenverkehr im Rahmen von VMware High Availability (HA), Migrationen, Klonen oder VMotion durchführen möchten, müssen Sie eine Verbindung konfigurieren, über die die verwalteten Hosts Daten empfangen können. Dafür müssen Sie folgende Ports freigeben:

- 443 (für Server-zu-Server-Migration- und Bereitstellungsdatenverkehr)
- 2050-5000 (für HA-Datenverkehr)
- 8000 (für VMotion)
- 8042-8045 (für HA-Datenverkehr)

Weitere Informationen zur Konfiguration der Ports erhalten Sie beim Firewalladministrator. Genauere Informationen zu Richtungsabhängigkeit und Protokollen für diese Ports finden Sie unter „TCP- und UDP-Ports für den Verwaltungszugriff“ auf Seite 193.

Öffnen von Firewallports für unterstützte Dienste und Verwaltungs-Agenten

Mit dem VI-Client können Sie die Firewall der Servicekonsole so konfigurieren, dass die allgemein unterstützten Dienste und installierten Verwaltungs-Agenten akzeptiert werden. Wenn Sie das Sicherheitsprofil des ESX Server 3-Hosts in VirtualCenter konfigurieren, werden durch das Hinzufügen oder Entfernen dieser Dienste oder Agenten automatisch festgelegte Ports geöffnet oder geschlossen, damit die Kommunikation mit dem Dienst oder dem Agenten möglich ist. Sie können folgende Dienste und Agenten hinzufügen oder entfernen:

- NIS-Client
- NFS-Client (unsicherer Dienst)
- SMB-Client (unsicherer Dienst)
- FTP-Client (unsicherer Dienst)
- SSH-Client
- Telnet-Client (unsicherer Dienst)
- NTP-Client
- iSCSI-Software-Client

- SSH-Server
- Telnet-Server (unsicherer Dienst)
- FTP-Server (unsicherer Dienst)
- NFS-Server (unsicherer Dienst)
- CIM-HTTP-Server (unsicherer Dienst)
- CIM-HTTPS-Server
- SNMP-Server
- Syslog-Client
- Andere unterstützte Verwaltungs-Agenten, die Sie installieren

---

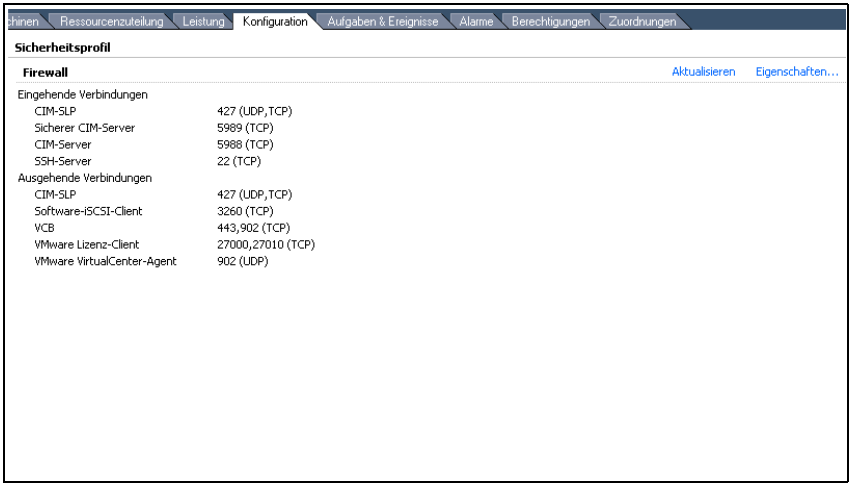
HINWEIS Die aufgeführten Dienste und Agenten können sich ändern, d. h. der VI-Client kann ggf. auch nicht aufgeführte Dienste und Agenten unterstützen. Außerdem werden nicht alle aufgeführten Dienste standardmäßig installiert. Zur Konfiguration und Aktivierung dieser Dienste sind gegebenenfalls weitere Schritte erforderlich.

Wenn Sie ein Gerät, einen Dienst oder einen Agenten installieren, der nicht in der Liste aufgeführt wurde, müssen Sie über die Befehlszeile Ports in der Firewall der Servicekonsole freigeben. Siehe „Konfiguration der Servicekonsolen-Firewall“ auf Seite 249.

So ermöglichen Sie einem Dienst oder Verwaltungs-Agenten den Zugriff auf ESX Server 3

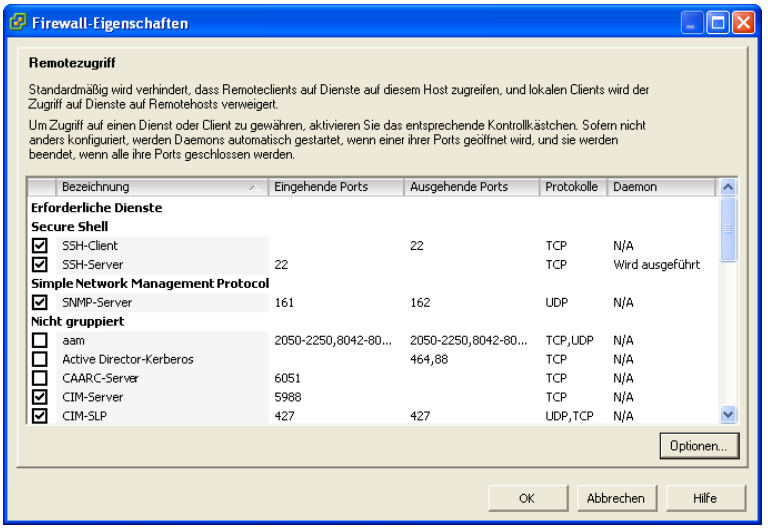
1. Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.
2. Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und dann auf **Sicherheitsprofil (Security Profile)**.

Der VI-Client zeigt eine Liste der gegenwärtig aktiven eingehenden und ausgehenden Verbindungen mit den entsprechenden Firewallports an.



3 Klicken Sie auf **Eigenschaften (Properties)**, um das Dialogfeld **Firewall-Eigenschaften (Firewall Properties)** zu öffnen.

Im Dialogfeld **Firewall-Eigenschaften (Firewall Properties)** werden alle Dienste und Verwaltungs-Agenten aufgelistet, die Sie für den Host konfigurieren können.


Firewall-Eigenschaften
Remotezugriff
Standardmäßig wird verhindert, dass Remoteclients auf Dienste auf diesem Host zugreifen, und lokalen Clients wird der Zugriff auf Dienste auf Remotehosts verweigert.
Um Zugriff auf einen Dienst oder Client zu gewähren, aktivieren Sie das entsprechende Kontrollkästchen. Sofern nicht anders konfiguriert, werden Daemons automatisch gestartet, wenn einer ihrer Ports geöffnet wird, und sie werden beendet, wenn alle ihre Ports geschlossen werden.
Bezeichnung
Eingehende Ports
Ausgehende Ports
Protokolle
Daemon
Erforderliche Dienste
Secure Shell
SSH-Client 22 TCP N/A
SSH-Server 22 TCP Wird ausgeführt
Simple Network Management Protocol
SNMP-Server 161 162 UDP N/A
Nicht gruppiert
aam 2050-2250,8042-80... 2050-2250,8042-80... TCP,UDP N/A
Active Director-Kerberos 464,88 TCP N/A
CAARC-Server 6051 TCP N/A
CIM-Server 5988 TCP N/A
CIM-SLP 427 427 UDP,TCP N/A
Optionen...
OK
Abbrechen
Hilfe

4 Wählen Sie die zu aktivierenden Dienste und Agenten.

Die Spalten **Eingehende Ports (Incoming Ports)** und **Ausgehende Ports (Outgoing Ports)** zeigen die Ports an, die der VI-Client für einen Dienst freigibt. Die Spalte **Protokoll (Protocol)** gibt das Protokoll an, das der Dienst verwendet, und die Spalte **Daemon** zeigt den Status des Daemons an, der dem Dienst zugewiesen wurde.

5 Klicken Sie auf **OK**.

Automatisieren des Dienstverhaltens basierend auf Firewalleinstellungen

ESX Server 3 kann automatisieren, ob Dienste basierend auf dem Status von Firewallports gestartet werden oder nicht. Eine solche Automatisierung sorgt dafür, dass die Dienste gestartet werden, wenn die Umgebung für ihre Aktivierung konfiguriert ist. Zum Beispiel kann die Situation vermieden werden, dass Dienste zwar gestartet werden, aber ihre Aufgabe aufgrund von geschlossenen Ports nicht ausführen können, indem ein Netzwerkdienst nur gestartet wird, wenn bestimmte Ports geöffnet sind.

Präzise Kenntnis der aktuellen Uhrzeit ist beispielsweise bei einigen Protokollen (z. B. Kerberos) eine Anforderung. Der NTP-Dienst kann präzise Zeitinformationen bereitstellen, doch dieser Dienst funktioniert nur, wenn die benötigten Ports in der Firewall geöffnet sind. Demzufolge kann der Dienst seine Aufgabe nicht erfüllen, wenn sämtliche Ports geschlossen sind. Der NTP-Dienst bietet eine Möglichkeit zum Konfigurieren der Bedingungen, unter denen der Dienst gestartet oder beendet werden kann. Diese Konfiguration umfasst Optionen, welche das Öffnen der entsprechenden Ports berücksichtigen, und startet und beendet den NTP-Dienst anschließend basierend auf diesen Bedingungen. Es sind mehrere Konfigurationsoptionen möglich, die alle auch für den SSH-Server gelten.

HINWEIS Die in diesem Abschnitt beschriebenen Einstellungen gelten nur für die über den VI-Client oder Anwendungen konfigurierten Diensteinstellungen, die mithilfe des VMware Infrastructure SDK erstellt wurden. Konfigurationen über andere Tools, z. B. das Dialogfeld **esxcfg-firewall** oder Konfigurationsdateien in `/etc/init.d/` sind von diesen Einstellungen nicht betroffen.

- **Automatisch starten, wenn ein Port geöffnet ist, und stoppen, wenn alle Ports geschlossen werden (Start automatically if any ports are open, and stop when all ports are closed)** – Die von VMware empfohlene Standardeinstellung für diese Dienste. Falls ein beliebiger Port geöffnet ist, versucht der Client die zum betreffenden Dienst gehörenden Netzwerkressourcen zu kontaktieren. Wenn einige Ports geöffnet sind, der Port für einen bestimmten Dienst jedoch geschlossen ist, misslingt der Versuch.Wird der zugehörige Port jedoch geöffnet**,** beginnt der Dienst seine Aufgaben zu erledigen**.**

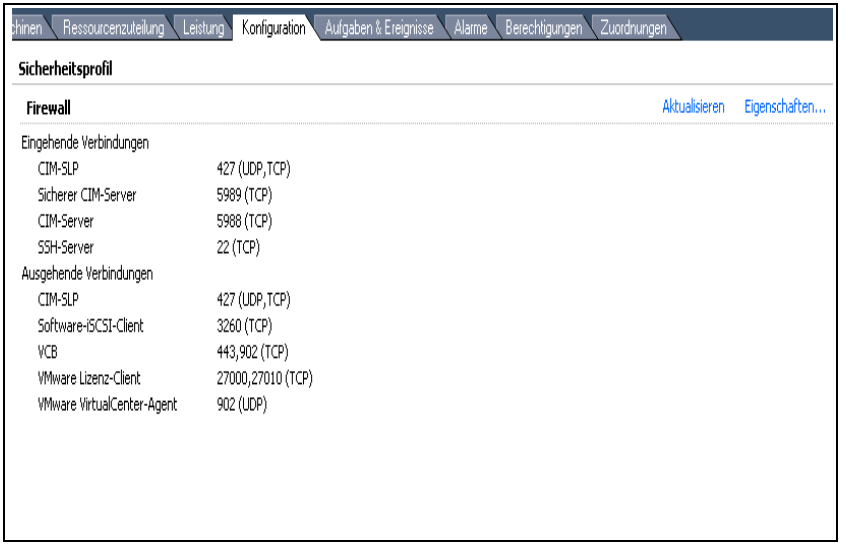
- **Mit dem Host starten und stoppen (Start and stop with host)** – Der Dienst wird kurz nach dem Starten des Hosts gestartet und kurz vor dessen Herunterfahren beendet. Ebenso wie **Automatisch starten, wenn ein Port geöffnet ist, und stoppen, wenn alle Ports geschlossen werden (Start automatically if any ports are open, and stop when all ports are closed)** bedeutet diese Option, dass der Dienst regelmäßig versucht, seine Aufgaben zu erledigen, z. B. beim NTP-Dienst das Kontaktieren des angegebenen NTP-Servers. Wenn der Port geschlossen war, später jedoch geöffnet wird, beginnt der Client unmittelbar mit der Erledigung seiner Aufgaben.
- **Manuell starten und stoppen (Start and stop manually)** – Der Host übernimmt die vom Benutzer festgelegten Diensteinstellungen unabhängig davon, welche Ports offen oder geschlossen sind. Wenn ein Benutzer den NTP-Dienst startet, wird dieser Dienst so lange ausgeführt, bis der Host ausgeschaltet wird. Wenn der Dienst gestartet und der Host ausgeschaltet wird, wird der Dienst als Teil des Herunterfahrens beendet. Sobald der Host jedoch eingeschaltet wird, wird auch der Dienst erneut gestartet, sodass der vom Benutzer festgelegte Status beibehalten bleibt.

So konfigurieren Sie das Verhältnis von Dienststart und Firewallkonfiguration

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

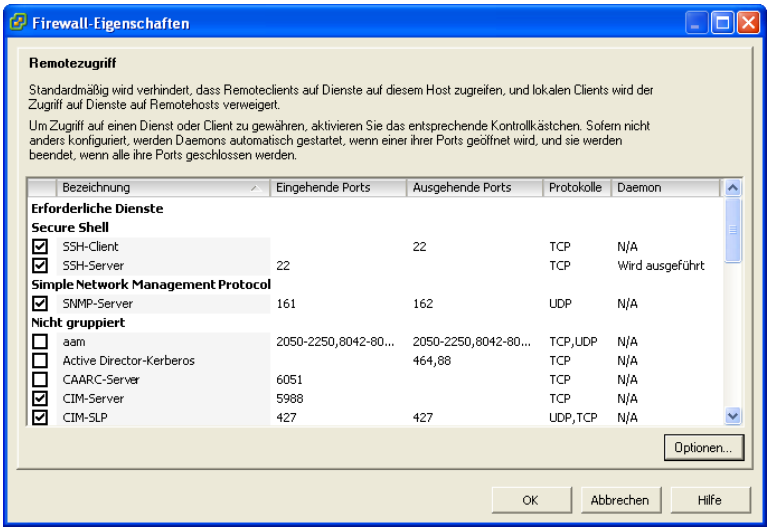
2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und dann auf **Sicherheitsprofil (Security Profile)**.

Der VI-Client zeigt eine Liste der gegenwärtig aktiven eingehenden und ausgehenden Verbindungen mit den entsprechenden Firewallports an.



3 Klicken Sie auf **Eigenschaften (Properties)**.

Im Dialogfeld **Firewall-Eigenschaften (Firewall Properties)** werden alle Dienste und Verwaltungs-Agenten aufgelistet, die Sie für den Host konfigurieren können.


Firewall-Eigenschaften
Remotezugriff
Standardmäßig wird verhindert, dass Remoteclients auf Dienste auf diesem Host zugreifen, und lokalen Clients wird der Zugriff auf Dienste auf Remotehosts verweigert.
Um Zugriff auf einen Dienst oder Client zu gewähren, aktivieren Sie das entsprechende Kontrollkästchen. Sofern nicht anders konfiguriert, werden Daemons automatisch gestartet, wenn einer ihrer Ports geöffnet wird, und sie werden beendet, wenn alle ihre Ports geschlossen werden.
Bezeichnung
Eingehende Ports
Ausgehende Ports
Protokolle
Daemon
Erforderliche Dienste
Secure Shell
SSH-Client 22 TCP N/A
SSH-Server 22 TCP Wird ausgeführt
Simple Network Management Protocol
SNMP-Server 161 162 UDP N/A
Nicht gruppiert
aam 2050-2250,8042-80... 2050-2250,8042-80... TCP,UDP N/A
Active Director-Kerberos 464,88 TCP N/A
CAARC-Server 6051 TCP N/A
CIM-Server 5988 TCP N/A
CIM-SLP 427 427 UDP,TCP N/A
Optionen...
OK
Abbrechen
Hilfe

4 Wählen Sie den Dienst aus, der konfiguriert werden soll, und klicken Sie auf **Optionen (Options)**.

Die Option **Startrichtlinie (Startup Policy)** legt fest, wann der Dienst gestartet wird. In diesem Dialogfeld finden Sie auch Informationen zum aktuellen Status des Dienstes und Optionen zum manuellen Starten, Beenden und Neustarten des Dienstes.

5 Wählen Sie unter **Startrichtlinie (Startup Policy)** eine Option aus.

6 Klicken Sie auf **OK**.

Absichern virtueller Maschinen durch VLANs

Das Netzwerk gehört zu den gefährdetsten Teilen eines jeden Systems. Ein virtuelles Netzwerk benötigt daher ebenso wie ein physisches Netzwerk Schutz. Wenn das Netzwerk virtueller Maschinen an ein physisches Netzwerk angeschlossen ist, kann es ebenso Sicherheitslücken aufweisen wie ein Netzwerk, das aus physischen Computern besteht. Selbst wenn das virtuelle Netzwerk nicht an ein physisches Netzwerk angeschlossen ist, kann ein Angriff auf virtuelle Maschinen innerhalb des Netzwerks von anderen virtuellen Maschinen des Netzwerks aus erfolgen. Die Anforderungen an die Absicherung virtueller Maschinen sind oft die gleichen wie für physische Maschinen.

Virtuelle Maschinen sind voneinander isoliert. Eine virtuelle Maschine kann weder Lese- noch Schreiboperationen im Speicher der anderen virtuellen Maschine ausführen noch auf deren Daten zugreifen, ihre Anwendungen verwenden usw. Im Netzwerk kann jedoch jede virtuelle Maschine oder eine Gruppe virtueller Maschinen Ziel eines unerlaubten Zugriffs von anderen virtuellen Maschinen sein und daher weiteren Schutzes durch externe Maßnahmen bedürfen. Dies können Sie durch folgende Maßnahmen erreichen:

- Hinzufügen von Firewallschutz für das virtuelle Netzwerk durch Installation und Konfiguration von Softwarefirewalls auf einigen oder allen virtuellen Maschinen im Netzwerk.

  Aus Effizienzgründen können Sie private Ethernet-Netzwerke virtueller Maschinen oder *Virtuelle Netzwerke* einrichten. Bei virtuellen Netzwerken installieren Sie eine Softwarefirewall auf einer virtuellen Maschine am Eingang des virtuellen Netzwerks. Diese dient als Schutzpufferzone zwischen dem physischen Netzwerkadapter und den übrigen virtuellen Maschinen im virtuellen Netzwerk.

  Die Installation einer Softwarefirewall auf virtuellen Maschinen am Eingang eines virtuellen Netzwerks ist eine bewährte Sicherheitsmaßnahme. Da jedoch Softwarefirewalls die Leistung verlangsamen können, sollten Sie Sicherheitsbedürfnisse und Leistungsanforderungen abwägen, bevor Sie Softwarefirewalls in anderen virtuellen Maschinen im Netzwerk installieren. Siehe „Übersicht über Netzwerkkonzepte“ auf Seite 20.

- Beibehalten verschiedener Zonen aus virtuellen Maschinen innerhalb eines Hosts auf verschiedenen Netzwerksegmenten. Wenn Sie virtuelle Maschinenzonen in deren eigenen Netzwerksegmenten isolieren, minimieren Sie das Risiko eines Datenverlusts aus einer virtuellen Maschinenzone in die nächste. Die Segmentierung verhindert mehrere Gefahren. Zu diesen Gefahren gehört auch die Manipulation des Adressauflösungsprotokolls (ARP), wobei der Angreifer die ARP-Tabelle so manipuliert, dass die MAC- und IP-Adressen neu zugeordnet werden, wodurch ein Zugriff auf den Netzwerkdatenverkehr vom und zum Host möglich ist. Angreifer verwenden diese ARP-Manipulierung für Denial of Service-Angriffe (DOS), zur Übernahme des Zielsystems und zur anderweitigen Beeinträchtigung des virtuellen Netzwerks.

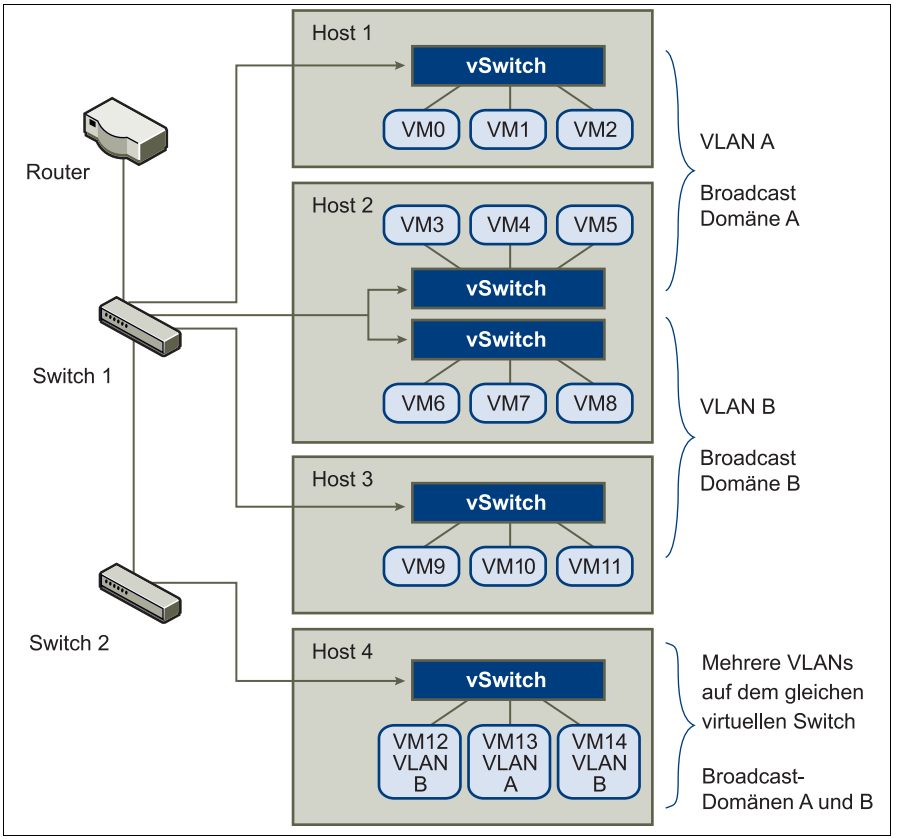
  Eine sorgfältige Planung der Segmentierung senkt das Risiko von Paketübertragungen zwischen virtuellen Maschinenzonen und somit von Spionageangriffen, die voraussetzen, dass dem Opfer Netzwerkdatenverkehr zugestellt wird. So kann ein Angreifer auch keinen unsicheren Dienst in einer virtuellen Maschinenzone aktivieren, um auf andere virtuelle Maschinenzonen im Host zuzugreifen. Sie können die Segmentierung mit einer der beiden folgenden Methoden herstellen, von denen jede andere Vorteile bietet.

- Verwenden Sie getrennte physische Netzwerkadapter für Zonen virtueller Maschinen, damit die Zonen auch tatsächlich voneinander getrennt sind. Die Beibehaltung getrennter physischer Netzwerkadapter für die virtuellen Maschinenzonen stellt unter Umständen die sicherste Methode dar, und gleichzeitig ist sie am wenigsten anfällig für Konfigurationsfehler nach dem Anlegen des ersten Segments.
- Richten Sie virtuelle LANs (VLANs) zur Absicherung des Netzwerks ein. Da VLANs fast alle Sicherheitsvorteile bieten, die auch die Implementierung physisch getrennter Netzwerke aufweist, ohne dass dafür der Mehraufwand an Hardware eines physischen Netzwerks notwendig ist, stellen sie eine rentable Lösung zur Verfügung, die die Kosten für die Bereitstellung und Wartung zusätzlicher Geräte, Kabel usw. einsparen kann.

VLANs sind eine Netzwerkarchitektur nach dem IEEE-Standard und verfügen über spezifische Kennzeichnungsmethoden, durch die Datenpakete nur an die Ports weitergeleitet werden, die zum VLAN gehören. Wenn das VLAN ordnungsgemäß konfiguriert ist, ist es ein zuverlässiges Mittel zum Schutz einer Gruppe virtueller Maschinen vor zufälligem und böswilligem Eindringen.

Mit VLANs können Sie ein physisches Netzwerk so in Segmente aufteilen, dass zwei Computer oder virtuelle Maschinen im Netzwerk nur dann Pakete untereinander austauschen können, wenn sie zum gleichen VLAN gehören. So gehören zum Beispiel Buchhaltungsunterlagen und -transaktionen zu den wichtigsten vertraulichen internen Informationen eines Unternehmens. Wenn in einem Unternehmen die virtuellen Maschinen der Verkaufs-, Logistik- und Buchhaltungsmitarbeiter an das gleiche physische Netzwerk angeschlossen sind, können Sie die virtuellen Maschinen für die Buchhaltungsabteilung schützen, indem Sie VLANs wie in Abbildung 10-4 einrichten.

Abbildung 10-4. Beispielplan eines VLAN



Bei dieser Konfiguration verwenden alle Mitarbeiter der Buchhaltungsabteilung virtuelle Maschinen im VLAN A, die Mitarbeiter der Vertriebsabteilung verwenden die virtuellen Maschinen im VLAN B.

Der Router leitet die Datenpakete mit Buchhaltungsdaten an die Switches weiter. Diese Pakete sind so gekennzeichnet, dass sie nur an VLAN A weitergeleitet werden dürfen. Daher sind die Daten auf die Broadcastdomäne A beschränkt und können nur an die Broadcastdomäne B weitergeleitet werden, wenn der Router entsprechend konfiguriert wurde.

Bei dieser VLAN-Konfiguration wird verhindert, dass Mitarbeiter des Vertriebs Datenpakete abfangen können, die für die Buchhaltungsabteilung bestimmt sind. Die Buchhaltungsabteilung kann zudem auch keine Datenpakete empfangen, die für den Vertrieb bestimmt sind. Virtuelle Maschinen, die an einen gemeinsamen virtuellen Switch angebunden sind, können sich dennoch in unterschiedlichen VLANs befinden.

Sicherheitsempfehlungen für vSwitches und VLANs

ESX Server 3 ist mit einer vollständigen VLAN-Implementierung nach IEEE 802.1q ausgestattet. Wie Sie die VLANs einrichten, um Teile eines Netzwerks abzusichern, hängt von Faktoren wie dem installierten Gastbetriebssystem, der Konfiguration der Netzwerkgeräte usw. ab. Zwar kann VMware keine spezifischen Empfehlungen aussprechen, wie die VLANs eingerichtet werden sollten, folgende Faktoren sollten jedoch berücksichtigt werden, wenn Sie VLANs als Teil der Sicherheitsrichtlinien einsetzen:

- **Setzen Sie VLANs im Rahmen eines Sicherheitspakets ein** – Mit VLANs kann effektiv gesteuert werden, wo und in welchem Umfang Daten im Netzwerk übertragen werden. Wenn ein Angreifer Zugang zum Netzwerk erlangt, wird der Angriff mit hoher Wahrscheinlichkeit nur auf das VLAN beschränkt, das als Zugangspunkt diente, wodurch das Risiko für das gesamte Netzwerk verringert wird.

  VLANs bieten nur dadurch Schutz, dass sie steuern, wie Daten weitergeleitet und verarbeitet werden, nachdem sie die Switches passiert haben und sich im Netzwerk befinden. Sie können VLANs dazu nutzen, die 2. Schicht des Netzwerkmodells, die Sicherungsschicht, zu schützen. Die Einrichtung von VLANs schützt jedoch weder die Bitübertragungsschicht noch die anderen Schichten. Auch bei der Verwendung von VLANs sollten Sie zusätzlichen Schutz durch Absicherung der Hardware (Router, Hubs usw.) und Verschlüsselung der Datenübertragungen implementieren.

  VLANs ersetzen Softwarefirewalls in den Konfigurationen virtueller Maschinen nicht. In den meisten Netzwerkkonfigurationen mit VLANs gibt es auch Softwarefirewalls. Wenn Sie VLANs in Ihr virtuelles Netzwerk implementieren, müssen die Firewalls VLANs erkennen können.

- **Stellen Sie sicher, dass die VLANs ordnungsgemäß konfiguriert sind** – Eine Fehlkonfiguration der Ausstattung und Netzwerkhardware, -firmware oder -software setzt ein VLAN möglichen VLAN-Hopping-Angriffen aus. VLAN-Hopping tritt dann auf, wenn ein Angreifer mit autorisiertem Zugriff auf ein VLAN Datenpakete erstellt, die die physischen Switches dazu bringen, die Pakete in ein anderes VLAN zu übertragen, für das der Angreifer keine Zugriffsberechtigung besitzt. Anfälligkeit für diese Art von Angriffen liegt meist dann vor, wenn ein Switch falsch für den nativen VLAN-Betrieb konfiguriert wurde, wodurch der Switch nicht gekennzeichnete Pakete empfangen und übertragen kann.

  Um ein VLAN-Hopping zu verhindern, aktualisieren Sie stets Ihre Umgebung, indem Sie Updates der Hardware und Firmware sofort aufspielen. Achten Sie bei der Konfiguration Ihrer Umgebung auch stets auf die Einhaltung der Empfehlungen des Herstellers.

Virtuelle Switches von VMware unterstützen nicht das Konzept nativer VLANs. Alle Daten, die über diese Switches übertragen werden, müssen ordnungsgemäß gekennzeichnet werden. Da es jedoch im Netzwerk auch andere Switches geben kann, die für den nativen VLAN-Betrieb konfiguriert wurden, können VLANs mit virtuellen Switches dennoch anfällig für VLAN-Hopping sein.

Wenn Sie VLANs zur Netzwerksicherung verwenden möchten, empfiehlt VMware, die native VLAN-Funktion für alle Switches zu deaktivieren, sofern nicht ein zwingender Grund vorliegt, dass einige VLANs im nativen Modus betrieben werden müssen. Wenn Sie ein natives VLAN verwenden müssen, beachten Sie die Konfigurationsrichtlinien des Switches-Herstellers für diese Funktion.

- **Richten Sie ein eigenes VLAN bzw. einen eigenen virtuellen Switch für die Kommunikation zwischen den Verwaltungsprogrammen und der Servicekonsole ein** – Sowohl bei der Verwendung eines Verwaltungs-Clients als auch der Befehlszeile werden alle Konfigurationsaufgaben für ESX Server 3, z. B. Speicher, Steuerungsaspekte des Verhaltens virtueller Maschinen oder die Einrichtung virtueller Switches oder Netzwerke, über die Servicekonsole ausgeführt. Da die Servicekonsole die Steuerungszentrale von ESX Server 3 ist, hat ihr Schutz vor Missbrauch oberste Priorität.

  Die Verwaltungsclients von VMware ESX Server 3 verwenden Authentifizierung und Verschlüsselung, um einen unerlaubten Zugriff auf die Servicekonsole zu verhindern. Andere Dienste bieten jedoch ggf. nicht den gleichen Schutz. Wenn Angreifer Zugriff auf die Servicekonsole erlangen, können sie viele Attribute des ESX Server 3-Hosts neu konfigurieren. So können Sie zum Beispiel die gesamte Konfiguration der virtuellen Switches oder die Autorisierungsverfahren usw. ändern.

  Die Netzwerkanbindung für die Servicekonsole wird über virtuelle Switches hergestellt. Um diese wichtigen ESX Server 3-Komponenten zu schützen, empfiehlt VMware die Isolierung der Servicekonsole durch eines der folgenden Verfahren:

  - Richten Sie ein VLAN für die Kommunikation der Verwaltungsprogramme mit der Servicekonsole ein.
  - Konfigurieren Sie den Netzwerkzugang für die Verwaltungsprogrammverbindungen mit der Servicekonsole über einen einzelnen virtuellen Switch und einen oder mehrere Uplink-Ports.

Beide Methoden verhindern, dass jemand ohne Zugriff auf das Servicekonsolen-VLAN oder den virtuellen Switch, den ein- und ausgehenden Datenverkehr der Servicekonsole verfolgen kann. Außerdem können so Angreifer keine Pakete an die Servicekonsole senden. Alternativ können Sie stattdessen die Servicekonsole in einem eigenen physischen Netzwerksegment konfigurieren. Die physische Segmentierung bietet eine gewisse zusätzliche Sicherheit, da diese vor einer späteren Fehlkonfiguration schützt.

Zusätzlich zur Einrichtung eines eigenen VLAN oder virtuellen Switches für die Kommunikation der Verwaltungsprogramme mit der Servicekonsole sollten Sie ein eigenes VLAN oder einen eigenen virtuellen Switch für VMotion und für Netzwerkspeicher einrichten.

Wenn Ihre Konfiguration ein iSCSI-SAN umfasst, das direkt über den Host und nicht durch den Hardware-Adapter konfiguriert wurde, sollten Sie einen eigenen virtuellen Switch einrichten, der eine gemeinsam genutzte Netzwerkkonnektivität für die Servicekonsole und für iSCSI bietet. Diese zweite Netzwerkverbindung für die Servicekonsole besteht zusätzlich zur primären Servicekonsolen-Netzwerkverbindung, die Sie für die Kommunikation Ihrer Verwaltungsprogramme verwenden. Die zweite Servicekonsolen-Netzwerkverbindung unterstützt nur die iSCSI-Aktivitäten, und Sie sollten Sie nicht für Verwaltungsaktivitäten oder die Verwaltungsprogrammkommunikation verwenden.

Schutz durch virtuelle Switches in VLANs

Die virtuellen Switches von VMware schützen gegen bestimmte Bedrohungen der VLAN-Sicherheit. Durch den Aufbau der virtuellen Switches schützen sie VLANs gegen viele Arten von Angriffen, die meist auf VLAN-Hopping basieren. Dieser Schutz garantiert jedoch nicht, dass Ihre virtuellen Maschinen gegen andere Arten von Angriffen immun sind. So schützen virtuelle Switches zum Beispiel nicht das physische Netzwerk vor diesen Angriffen, sondern nur das virtuelle Netzwerk.

Die folgende Liste vermittelt Ihnen die Grundlagen zu einigen Angriffsarten, gegen die virtuelle Switches und VLANs schützen können.

- **MAC-Flooding** – Diese Angriffe überschwemmen den Switch mit Datenpaketen, die MAC-Adressen enthalten, die als von verschiedenen Quellen stammend gekennzeichnet wurden. Viele Switches verwenden eine assoziative Speichertabelle (CAM-Tabelle), um die Quelladresse für jedes Datenpaket zu speichern. Wenn die Tabelle voll ist, schaltet der Switch ggf. in einen vollständig geöffneten Status um, in dem alle eingehenden Pakete auf allen Ports übertragen werden, sodass der Angreifer den gesamten Datenverkehr des Switches verfolgen kann. In diesem Fall kann es auch zu Paketlecks in andere VLANs kommen.

Zwar speichern die virtuellen Switches von VMware eine MAC-Adressentabelle, aber sie erhalten die MAC-Adressen nicht von erkennbarem Datenverkehr und sind daher gegen diese Art von Angriffen immun.

- **Angriffe durch 802.1q- und ISL-Kennzeichnung** – Bei diesem Angriff werden die Datenblöcke durch den Switch an ein anderes VLAN weitergeleitet, indem der Switch durch einen Trick dazu gebracht wird, als Trunk zu fungieren und den Datenverkehr an andere VLANs weiterzuleiten.

  Die virtuellen Switches von VMware führen das dynamische Trunking, das für diese Art des Angriffs notwendig ist, nicht aus, und sind daher immun.

- **Doppelt eingekapselte Angriffe** – Bei dieser Art von Angriffen erstellt der Angreifer ein doppelt eingekapseltes Paket, in dem sich der VLAN-Bezeichner im inneren Tag vom VLAN-Bezeichner im äußeren Tag unterscheidet. Um Rückwärtskompatibilität zu gewährleisten, entfernen native VLANs standardmäßig das äußere Tag von übertragenen Paketen. Wenn ein nativer VLAN-Switch das äußere Tag entfernt, bleibt nur das innere Tag übrig, welches das Paket zu einem anderen VLAN weiterleitet, als im jetzt fehlenden äußeren Tag angegeben war.

  Die virtuellen Switches von VMware verwerfen alle doppelt eingekapselten Datenblöcke, die eine virtuelle Maschine auf einem für ein bestimmtes VLAN konfigurierten Port senden möchte. Daher sind sie immun gegen diese Art von Angriffen.

- **Multicast-Brute-Force-Angriffe** – Bei diesen Angriffen wird eine große Anzahl an Multicast-Datenblöcken fast zeitgleich an ein bekanntes VLAN gesendet, um den Switch zu überfordern, sodass er versehentlich einige Datenblöcke in andere VLANs überträgt.

  Die virtuellen Switches von VMware erlauben es Datenblöcken nicht, ihren richtigen Übertragungsbereich (VLAN) zu verlassen und sind daher gegen diese Art von Angriffen immun.

- **Spanning-Tree-Angriffe** – Diese Angriffe zielen auf das Spanning-Tree-Protokoll (STP), das zur Steuerung der Überbrückung verschiedener Teile des LANs verwendet wird. Der Angreifer sendet Pakete der Bridge Protocol Data Unit (BPDU) in dem Versuch, die Netzwerktopologie zu ändern und sich selbst als Root-Bridge einzusetzen. Als Root-Bridge kann der Angreifer dann die Inhalte übertragener Datenblöcke mitschneiden.

  Die virtuellen Switches von VMware unterstützen STP nicht und sind daher gegen diese Art von Angriffen immun.

- **Zufallsdatenblock-Angriffe** – Bei diesen Angriffen wird eine große Anzahl an Paketen, bei denen die Quell- und Zieladressen gleich sind, die jedoch Felder unterschiedlicher Länge, Art und mit verschiedenem Inhalt enthalten, versendet. Ziel des Angriffes ist es zu erzwingen, dass Pakete versehentlich in ein anderes VLAN fehlgeleitet werden.

  Die virtuellen Switches von VMware sind gegen diese Art von Angriffen immun.

Da mit der Zeit immer neue Sicherheitsgefahren auftreten, kann diese Liste möglicher Angriffe nicht vollständig sein. Konsultieren Sie regelmäßig die VMware-Sicherheitsressourcen im Internet (http://www.vmware.com/support/security.html), um mehr über Sicherheit, neue Sicherheitswarnungen und die Sicherheitstaktik von VMware zu erfahren.

Absichern der Ports virtueller Switches

Wie bei physischen Netzwerkadaptern kann ein virtueller Netzwerkadapter Datenblöcke versenden, die von einer anderen virtuellen Maschine zu stammen scheinen oder eine andere virtuelle Maschine imitieren, damit er Datenblöcke aus dem Netzwerk empfangen kann, die für die jeweilige virtuelle Maschine bestimmt sind. Außerdem kann ein virtueller Netzwerkadapter, genauso wie ein physischer Netzwerkadapter, so konfiguriert werden, dass er Datenblöcke empfängt, die für andere virtuelle Maschinen bestimmt sind.

Wenn Sie einen virtuellen Switch für Ihr Netzwerk erstellen, fügen Sie Portgruppen hinzu, um für die an den Switch angeschlossenen virtuellen Maschinen, Speichersysteme usw. Richtlinien zu konfigurieren. Virtuelle Ports werden über den VI-Client erstellt.

Während des Hinzufügens eines Ports oder einer Portgruppe zu einem virtuellen Switch konfiguriert der VI-Client ein Sicherheitsprofil für den Port. Mit diesem Sicherheitsprofil können Sie sicherstellen, dass ESX Server 3 verhindert, dass die Gastbetriebssysteme auf den virtuellen Maschinen andere Computer im Netzwerk imitieren können. Diese Sicherheitsfunktion wurde so implementiert, dass das Gastbetriebssystem, welches für die Imitation verantwortlich ist, nicht erkennt, dass diese verhindert wurde.

Das Sicherheitsprofil bestimmt, wie streng der Schutz gegen Imitierungs- oder Abfangangriffe auf virtuelle Maschinen sein soll. Damit Sie die Einstellungen des Sicherheitsprofils richtig anwenden können, benötigen Sie Grundkenntnisse darüber, wie virtuelle Netzwerkadapter Datenübertragungen steuern und wie Angriffe auf dieser Ebene vorgenommen werden.

Jedem virtuellen Netzwerkadapter wird bei seiner Erstellung eine eindeutige MAC-Adresse zugewiesen. Diese Adresse wird „Ursprünglich zugewiesene MAC-Adresse“ genannt. Obwohl die ursprüngliche MAC-Adresse von außerhalb des Gastbetriebssystems neu konfiguriert werden kann, kann sie nicht vom

Gastbetriebssystem selbst geändert werden. Außerdem verfügt jeder Adapter über eine geltende MAC-Adresse, die eingehenden Netzwerkverkehr mit einer MAC-Adresse, die nicht der geltenden MAC-Adresse entspricht, herausfiltert. Das Gastbetriebssystem ist für die Einstellung der geltenden MAC-Adresse verantwortlich. In der Regel stimmen die geltende MAC-Adresse und die ursprünglich zugewiesene MAC-Adresse überein.

Beim Versand von Datenpaketen schreibt das Betriebssystem die geltende MAC-Adresse des eigenen Netzwerkadapters in das Feld mit der Quell-MAC-Adresse des Ethernet-Frames. Es schreibt auch die MAC-Adresse des Empfänger-Netzwerkadapters in das Feld mit der Ziel-MAC-Adresse. Der empfangende Adapter akzeptiert Datenpakete nur dann, wenn die Ziel-MAC-Adresse im Paket mit seiner eigenen geltenden MAC-Adresse übereinstimmt.

Bei der Erstellung stimmen die geltende und die ursprünglich zugewiesene MAC-Adresse überein. Das Betriebssystem der virtuellen Maschine kann die geltenden MAC-Adresse jedoch jederzeit auf einen anderen Wert setzen. Wenn ein Betriebssystem die geltenden MAC-Adresse ändert, empfängt der Netzwerkadapter Netzwerkdatenverkehr, der für die neue MAC-Adresse bestimmt ist. Das Betriebssystem kann jederzeit Frames mit einer imitierten Quell-MAC-Adresse senden. Daher kann ein Betriebssystem böswillige Angriffe auf die Geräte in einem Netzwerk durchführen, indem es einen Netzwerkadapter imitiert, der vom Empfängernetzwerk autorisiert wurde.

Mit den Sicherheitsprofilen für den virtuellen Switch auf den ESX Server 3-Hosts können Sie sich gegen diese Art von Angriffen schützen, indem Sie drei Optionen einstellen:

- **MAC-Adressänderungen** – In der Standardeinstellung ist diese Option auf **Akzeptieren (Accept)** festgelegt, d. h. dass der ESX Server 3-Host Anforderungen, die geltende MAC-Adresse in eine andere als die ursprünglich zugewiesene Adresse zu ändern, akzeptiert. Die Einstellung der Option **MAC-Adressenänderungen (MAC Address Changes)** beeinflusst den Datenverkehr, den eine virtuelle Maschine empfängt.

  Zum Schutz gegen MAC-Imitation können Sie diese Option auf **Ablehnen (Reject)** einstellen. In diesem Fall lehnt der ESX Server 3-Host alle Anforderungen, die geltende MAC-Adresse in eine andere als die ursprünglich zugewiesene Adresse zu ändern, ab. Stattdessen wird der Port, der von dem virtuellen Adapter zum Senden der Anforderung verwendet wird, deaktiviert. Als Folge erhält der virtuelle Adapter keine weiteren Datenpakete mehr, bis er die geltende MAC-Adresse ändert, sodass sie mit der ursprünglichen MAC-Adresse übereinstimmt. Das Gastbetriebssystem erkennt nicht, dass die Änderung der MAC-Adresse nicht angenommen wurde.

HINWEIS In bestimmten Situationen ist es tatsächlich notwendig, dass mehrere Adapter in einem Netzwerk die gleiche MAC-Adresse haben, zum Beispiel wenn Sie des Microsoft-Netzwerklastenausgleichs im Unicast-Modus verwenden. Bei Verwendung von des Microsoft-Netzwerklastenausgleichs im Standard-Multicast-Modus haben die Adapter nicht die gleiche MAC-Adresse.

- **Gefälschte Übertragungen** – In der Standardeinstellung ist diese Option auf **Akzeptieren (Accept)** festgelegt, d. h. der ESX Server 3-Host vergleicht die Quell- und die geltende MAC-Adresse nicht. Die Einstellung der Option **Gefälschte Übertragungen (Forged Trasmits)** ändert den Datenverkehr, der von einer virtuellen Maschine versandt wird.

  Zum Schutz gegen MAC-Imitation können Sie diese Option auf **Ablehnen (Reject)** einstellen. In diesem Fall vergleicht der ESX Server 3-Host die Quell-MAC-Adresse, die vom Betriebssystem übertragen wird, mit der geltenden MAC-Adresse des Adapters, um festzustellen, ob sie übereinstimmen. Wenn die Adressen nicht passen, verwirft der ESX Server 3 das Paket.

  Das Gastbetriebssystem erkennt nicht, dass der virtuelle Netzwerkadapter die Pakete mit der imitierten MAC-Adresse nicht senden kann. Der ESX Server 3-Host fängt alle Pakete mit imitierten Adressen vor der Übermittlung ab. Das Gastbetriebssystem geht ggf. davon aus, dass die Pakete verworfen wurden.

- **Betrieb im Promiscuous-Modus** – In der Standardeinstellung ist diese Option auf **Ablehnen (Reject)** festgelegt, d. h. der virtuelle Netzwerkadapter kann nicht im Promiscuous-Modus betrieben werden. Der Promiscuous-Modus deaktiviert jegliche Empfangsfilterung, die der virtuelle Netzwerkadapter normalerweise ausführen würde, sodass das Gastbetriebssystem den gesamten Datenverkehr aus dem Netzwerk empfängt.

  Zwar kann der Promiscuous-Modus für die Nachverfolgung von Netzwerkaktivitäten nützlich sein, aber er ist ein unsicherer Betriebsmodus, da jeder Adapter im Promiscuous-Modus Zugriff auf alle Pakete hat, auch wenn manche Pakete nur für einen spezifischen Netzwerkadapter bestimmt sind. Das bedeutet, dass ein Administrator oder Root-Benutzer in einer virtuellen Maschine rein theoretisch den Datenverkehr, der für andere Gast- oder Hostbetriebssysteme bestimmt ist, einsehen kann.

HINWEIS Unter bestimmten Umständen ist es notwendig, einen virtuellen Switch in den Promiscuous-Modus zu setzen, zum Beispiel wenn Sie eine Software zur Netzwerkeinbruchserkennung oder einen Paketmitschneider verwenden.

Wenn Sie eine dieser Standardeinstellungen für einen Port ändern möchten, müssen Sie das Sicherheitsprofil in den Einstellungen des virtuellen Switches im VI-Client ändern. Informationen zum Bearbeiten dieser Einstellungen finden Sie unter „Richtlinien für virtuelle Switches“ auf Seite 51.

Absichern von iSCSI-Speicher

Der Speicher, den Sie für einen ESX Server 3-Host konfigurieren, kann ein oder mehrere SANs (Speichernetzwerke) umfassen, die iSCSI verwenden. iSCSI ist ein Instrument für den Zugriff auf SCSI-Geräte und zum Austausch von Datensätzen, indem das TCP/IP-Protokoll über einen Netzwerkport und nicht über einen direkten Anschluss an ein SCSI-Gerät eingesetzt wird. In iSCSI-Übertragungen werden Raw-SCSI-Datenblöcke in iSCSI-Datensätze eingekapselt und an das Gerät oder den Benutzer, das/der die Anforderung gestellt hat, übertragen.

iSCSI-SANs ermöglichen die effiziente Verwendung bestehender Ethernet-Infrastrukturen zum Zugriff auf Speicherressourcen durch ESX Server 3-Hosts, die diese Ressourcen dynamisch teilen können. Deshalb bieten iSCSI-SANs eine wirtschaftliche Speicherlösung für Umgebungen, die auf einem gemeinsamen Speicherpool für verschiedene Benutzer basieren. Wie in allen vernetzten Systemen sind auch iSCSI-SANs anfällig für Sicherheitsverletzungen. Wenn Sie iSCSI auf einem ESX Server 3-Host konfigurieren, können Sie diese Sicherheitsrisiken durch verschiedene Maßnahmen minimieren.

HINWEIS Die Anforderungen und Vorgehensweisen für die Absicherung von iSCSI-SANs ähneln denen für Hardware-iSCSI-Adapter, die Sie für ESX Server 3-Hosts und für iSCSI, das direkt über den ESX Server 3-Host konfiguriert wird, verwenden. Weitere Informationen zur Konfiguration von iSCSI-Adaptern und -Speichern finden Sie unter „iSCSI-Speicher“ auf Seite 116.

Absichern von iSCSI-Geräten über Authentifizierung

iSCSI-Geräte können gegen ungewollten Zugriff abgesichert werden, indem der ESX Server 3-Host (der *Initiator*) vom iSCSI-Gerät (dem *Ziel*) authentifiziert werden muss, wenn der Host versucht auf Daten in der Ziel-LUN zuzugreifen. Ziel der Authentifizierung ist es zu überprüfen, dass der Initiator das Recht hat, auf ein Ziel zuzugreifen. Dieses Recht wird bei der Konfiguration der Authentifizierung gewährt.

Sie haben zwei Möglichkeiten, wenn Sie die Authentifizierung für iSCSI-SANs auf dem ESX Server 3-Host einrichten:

- **Challenge Handshake Authentication Protocol (CHAP)** – Sie können das iSCSI-SAN so konfigurieren, dass die CHAP-Authentifizierung verwendet wird. Bei der CHAP-Authentifizierung sendet das iSCSI-Ziel, wenn der Initiator mit ihm Kontakt aufnimmt, einen vordefinierten ID-Wert und einen Zufallswert, den *Schlüssel*, an den Initiator. Der Initiator erstellt dann einen unidirektionalen Prüfsummenwert, den er an das Ziel sendet. Die Prüfsumme enthält drei Elemente: einen vordefinierten ID-Wert, den Zufallswert, den das Ziel gesendet hat, und einen privaten Wert, den sog. *CHAP-Schlüssel*, den sowohl der Initiator als auch das Ziel haben. Wenn das Ziel die Prüfsumme vom Initiator erhält, erstellt es aus den gleichen Elementen seine eigene Prüfsumme und vergleicht diese mit dem Prüfsummenwert des Initiators. Wenn die Ergebnisse übereinstimmen, authentifiziert das Ziel den Initiator.

  ESX Server 3 unterstützt die unidirektionale CHAP-Authentifizierung für iSCSI. Bidirektionales CHAP wird nicht unterstützt. Bei der unidirektionalen CHAP-Authentifizierung authentifiziert das Ziel den Initiator, nicht jedoch der Initiator das Ziel. Der Initiator verfügt nur über einen Satz von Anmeldedaten, der von allen iSCSI-Zielen verwendet wird.

  ESX Server 3 unterstützt die CHAP-Authentifizierung nur auf HBA-Ebene. Die zielbasierte CHAP-Authentifizierung, bei der verschiedene Anmeldedaten für die Ziele erstellt werden können, um eine bessere Zielunterscheidung vornehmen zu können, wird nicht unterstützt.

- **Deaktiviert** – Sie können das iSCSI-SAN so konfigurieren, dass keine Authentifizierung verwendet wird. Der Datenverkehr zwischen Initiator und Ziel wird dennoch rudimentär überprüft, da iSCSI-Zielgeräte normalerweise so eingerichtet sind, dass sie nur mit bestimmten Initiatoren kommunizieren.

  Die Deaktivierung einer strengeren Authentifizierung kann zum Beispiel sinnvoll sein, wenn sich der iSCSI-Speicher an einem Standort befindet und ein dediziertes Netzwerk oder VLAN für alle iSCSI-Geräte erstellt wird. Die iSCSI-Konfiguration ist sicher, weil sie von ungewolltem Zugriff isoliert ist, wie dies auch in einem Fibre-Channel-SAN der Fall wäre.

  Deaktivieren Sie die Authentifizierung grundsätzlich nur dann, wenn Sie einen Angriff auf das iSCSI-SAN riskieren können oder Probleme beheben müssen, die durch menschliches Versagen entstanden sind.

ESX Server 3 unterstützt für iSCSI weder Kerberos noch Secure Remote Protocol (SRP) noch Authentifizierungsverfahren mit öffentlichen Schlüsseln. Außerdem unterstützt es keine IPsec-Authentifizierung und -Verschlüsselung.

Mit dem VI-Client können Sie bestimmen, ob die Authentifizierung derzeit verwendet wird, und das Authentifizierungsverfahren konfigurieren.

So überprüfen Sie das Authentifizierungsverfahren

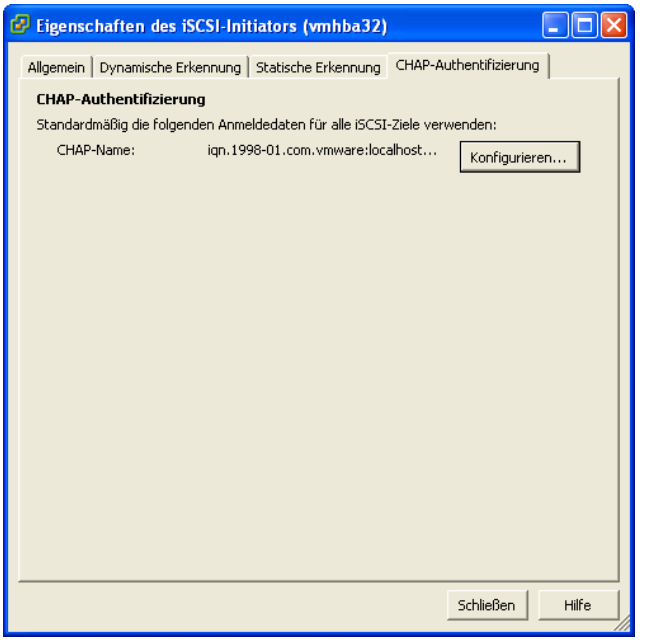
1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Speicheradapter (Storage Adapters)**.

3 Markieren Sie den zu überprüfenden iSCSI-Adapter, und klicken Sie dann auf **Eigenschaften (Properties)**. Das Dialogfeld **Eigenschaften des iSCSI-Initiators (iSCSI Initiator Properties)** wird geöffnet.

4 Klicken Sie auf **CHAP-Authentifizierung (CHAP Authentication)**.

Wenn unter **CHAP-Name (CHAP Name)** ein Name angezeigt wird (normalerweise der iSCSI-Initiatorname), verwendet das iSCSI-SAN die CHAP-Authentifizierung.



HINWEIS Wenn unter **CHAP-Name (CHAP Name) Keine Angabe (Not Specified)** angezeigt wird, verwendet das iSCSI-SAN nicht die CHAP/Authentifizierung.

5 Klicken Sie auf **Schließen (Close)**.

So konfigurieren Sie iSCSI für die CHAP-Authentifizierung

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

2 Klicken Sie auf die Registerkarte**Konfiguration (Configuration)** und anschließend auf **Speicheradapter (Storage Adapters)**.

3 Markieren Sie den gewünschten iSCSI-Adapter und klicken Sie dann auf **Eigenschaften (Properties)**. Das Dialogfeld **Eigenschaften des iSCSI-Initiators (iSCSI Initiator Properties)** wird geöffnet.

4 Klicken Sie auf **CHAP-Authentifizierung (CHAP Authentication)** > **Konfigurieren (Configure)**. Das Dialogfeld **CHAP-Authentifizierung (CHAP Authentication)** wird geöffnet.

5 Klicken Sie auf **Folgende CHAP-Anmeldeinformationen verwenden (Use the following CHAP credentials)**.

6 Führen Sie einen der folgenden Schritte aus:

- Wenn der CHAP-Name dem iSCSI-Adapternamen entsprechen soll, aktivieren Sie das Kontrollkästchen **Initiatornamen verwenden (Use initiator name)**.
- Um den CHAP-Namen nicht mit dem iSCSI-Adapternamen zu vergeben, dürfen Sie nicht **Initiatornamen verwenden (Use initiator name)** auswählen und müssen stattdessen einen Namen mit bis zu 255 alphanumerischen Zeichen in das Feld **CHAP-Name (CHAP Name)** eingeben.

7 Geben Sie einen CHAP-Schlüssel ein, der als Teil der Authentifizierung verwendet werden soll.

Der Schlüssel, den Sie eingeben, ist eine Zeichenfolge.

Der VI-Client verlangt keine Mindest- oder Höchstlänge für den CHAP-Schlüssel, den Sie eingeben. Bestimmte iSCSI-Speichergeräte fordern jedoch eine Mindestlänge oder beschränken die Art der verwendbaren Zeichen. Weitere Informationen zu den Anforderungen der Speichergeräte erhalten Sie in der Dokumentation des Herstellers.

8 Klicken Sie auf **OK**.

So deaktivieren Sie die iSCSI-Authentifizierung

1 Melden Sie sich am VI-Client an, und klicken Sie im Bestandslistenfenster auf den Server.

2 Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und anschließend auf **Speicheradapter (Storage Adapters)**.

3 Markieren Sie den gewünschten iSCSI-Adapter und klicken Sie dann auf **Eigenschaften (Properties)**. Das Dialogfeld **Eigenschaften des iSCSI-Initiators (iSCSI Initiator Properties)** wird geöffnet.

4 Klicken Sie auf **CHAP-Authentifizierung (CHAP Authentication)** > **Konfigurieren (Configure)**. Das Dialogfeld **CHAP-Authentifizierung (CHAP Authentication)** wird geöffnet.

5 Aktivieren Sie das Kontrollkästchen **CHAP-Authentifizierung deaktivieren (Disable CHAP authentication)**.

6 Klicken Sie auf **OK**.

Schützen eines iSCSI-SAN

Bei der Planung der iSCSI-Konfiguration sollten Sie Maßnahmen zur Verbesserung der allgemeinen Sicherheit des iSCSI-SAN ergreifen. Die iSCSI-Konfiguration ist nur so sicher wie das IP-Netzwerk. Wenn Sie also hohe Sicherheitsstandards bei der Netzwerkeinrichtung befolgen, schützen Sie auch den iSCSI-Speicher.

Hier sind einige spezifische Vorschläge zur Absicherung:

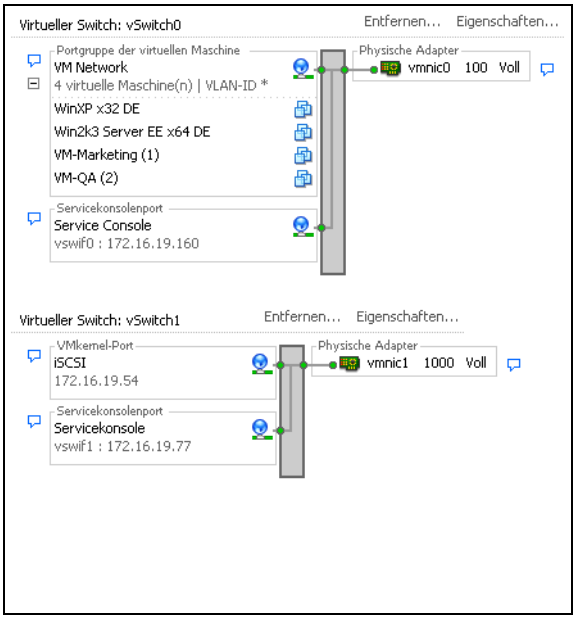
- **Schützen Sie übertragene Daten** – Eines der Hauptrisiken bei iSCSI-SANs ist, dass der Angreifer übertragene Speicherdaten mitschneiden kann.

  VMware empfiehlt zusätzliche Maßnahmen zu ergreifen, um zu verhindern, dass Angreifer iSCSI-Daten sehen können. Weder der Hardware-iSCSI-Adapter noch der ESX Server-Host iSCSI-Initiator verschlüsseln die Daten, die zu und von den Zielen übertragen werden, wodurch die Daten anfälliger für Mitschneideangriffe sind.

Wenn die virtuellen Maschinen die gleichen virtuellen Switches und VLANs wie die iSCSI-Struktur verwenden, ist der iSCSI-Datenverkehr potenziell dem Missbrauch durch Angreifer der virtuellen Maschinen ausgesetzt. Um sicherzustellen, dass Angreifer die iSCSI-Übertragungen nicht überwachen können, achten Sie darauf, dass keine Ihrer virtuellen Maschinen das iSCSI-Speichernetzwerk sehen kann.

Wenn Sie einen Hardware-iSCSI-Adapter verwenden, erreichen Sie dies, indem Sie sicherstellen, dass der iSCSI-Adapter und der physische Netzwerkadapter des ESX Server 3 nicht versehentlich außerhalb des Hosts durch eine gemeinsame Verwendung des Switches oder in anderer Form verbunden sind. Wenn Sie iSCSI direkt über den ESX Server 3-Host konfigurieren, können Sie dies erreichen, indem Sie den iSCSI-Speicher über einen anderen virtuellen Switch konfigurieren, als denjenigen, der durch Ihre virtuellen Maschinen verwendet wird (siehe Abbildung 10-5).

Abbildung 10-5. iSCSI-Speicher an einem eigenen virtuellen Switch



Wenn Sie iSCSI direkt über den Host und nicht über den Hardware-Adapter konfigurieren, müssen Sie beim Einrichten des virtuellen Netzwerks zwei Netzwerkverbindungen für die Servicekonsole anlegen. Dazu konfigurieren Sie die erste Netzwerkverbindung der Servicekonsole auf deren eigenem virtuellen Switch und verwenden diese ausschließlich für die Konnektivität der Verwaltungsprogramme (vSwitch 0 in der Abbildung). Dann konfigurieren

Sie die zweite Netzwerkverbindung für die Servicekonsole, damit sie den virtuellen Switch verwendet, den Sie für die iSCSI-Konnektivität nutzen (vSwitch 2 in der Abbildung). Die zweite Servicekonsolen-Netzwerkverbindung unterstützt nur die iSCSI-Aktivitäten, und Sie sollten Sie nicht für Verwaltungsaktivitäten oder die Verwaltungsprogrammkommunikation verwenden. Wenn Sie eine gewisse Trennung zwischen iSCSI und der Servicekonsole auf dem gemeinsam genutzten virtuellen Switch herstellen möchten, können Sie sie auf unterschiedlichen VLANs konfigurieren.

HINWEIS Konfigurieren Sie nicht das Standard-Gateway für die Servicekonsole auf dem virtuellen Switch, den Sie für die iSCSI-Konnektivität verwenden. Konfigurieren Sie es stattdessen auf dem virtuellen Switch, den Sie für die Konnektivität der Verwaltungsprogramme verwenden.

Zusätzlich zum Schutz durch einen eigenen virtuellen Switch können Sie das iSCSI-SAN durch die Konfiguration eines eigenen VLAN für das iSCSI-SAN schützen. Wenn die iSCSI-Konfiguration sich in einem eigenen VLAN befindet, wird sichergestellt, dass keine Geräte außer dem iSCSI-Adapter Einblick in Übertragungen im iSCSI-SAN haben.

- **Schützen Sie die iSCSI-Ports** – Wenn Sie die iSCSI-Geräte ausführen, öffnet der ESX Server 3-Host keine Ports, die Netzwerkverbindungen überwachen. Dadurch wird die Chance, dass ein Angreifer über ungenutzte Ports in den ESX Server 3-Host einbrechen und Kontrolle über ihn erlangen kann. Daher stellt der Betrieb von iSCSI kein zusätzliches Sicherheitsrisiko für den ESX Server 3-Host dar.

  Beachten Sie, dass auf jedem iSCSI-Zielgerät mindestens ein freigegebener TCP-Port für iSCSI-Verbindungen vorhanden sein muss. Wenn es Sicherheitsprobleme in der Software des iSCSI-Geräts gibt, können die Daten unabhängig von ESX Server 3 in Gefahr sein. Installieren Sie alle Sicherheitspatches des Speicherherstellers, und beschränken Sie die Anzahl der an das iSCSI-Netzwerk angeschlossenen Geräte, um dieses Risiko zu verringern.

Authentifizierung und Benutzerverwaltung 11

In diesem Kapitel wird erläutert, wie ESX Server 3 die Benutzerauthentifizierung vornimmt und wie Sie Benutzer- und Gruppenberechtigungen einrichten. Außerdem werden die Verschlüsselung für Verbindungen zum VI-Client, zum SDK und zu VI Web Access sowie die Konfigurierung eines delegierten Benutzernamens für Übertragungen bei NFS-Speichern erläutert.

In diesem Kapitel werden folgende Themen behandelt:

- „Absichern von ESX Server 3 über Authentifizierung und Berechtigungen“ auf Seite 221
- „Verschlüsselungs- und Sicherheitszertifikate für ESX Server 3“ auf Seite 236
- „Delegierte VM-Benutzer für NFS-Speicher“ auf Seite 242

Absichern von ESX Server 3 über Authentifizierung und Berechtigungen

ESX Server verwendet die PAM-Struktur (Pluggable Authentication Modules) zur Authentifizierung, wenn Benutzer über den VI-Client, VI Web Access oder die Servicekonsole auf den ESX Server 3-Host zugreifen. Die PAM-Konfiguration für VMware-Dienste befindet sich unter `/etc/pam.d/vmware-authd`, in der die Verzeichnispfade zu Authentifizierungsmodulen gespeichert sind.

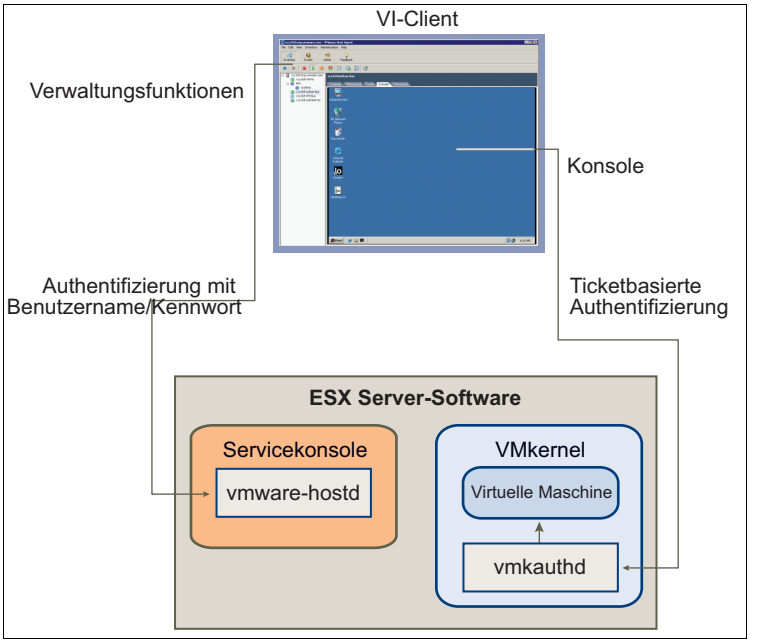
Die Standardinstallation von ESX Server 3 verwendet wie Linux die `/etc/passwd`-Authentifizierung. Sie können ESX Server 3 jedoch auch so konfigurieren, dass eine andere verteilte Authentifizierungsmethode verwendet wird. Wenn Sie statt der Standardimplementierung von ESX Server 3 ein Authentifizierungsprogramm eines anderen Anbieters verwenden möchten, finden Sie Anleitungen dazu in der

Dokumentation des entsprechenden Anbieters. Gegebenenfalls müssen Sie während der Einrichtung der Authentifizierung eines anderen Anbieters die Datei `/etc/pam.d/vmware-authd` mit neuen Modulinformationen aktualisieren.

Immer wenn sich ein VI-Client- oder VirtualCenter-Benutzer mit einem ESX Server 3-Host verbindet, stellt der Prozess `xinetd` eine Verbindung mit dem Prozess „VMware Host Agent (`vmware-hostd`)“ her. Der Prozess `vmware-hostd` empfängt den Benutzernamen und das Kennwort vom Client und leitet diese Daten zum PAM-Modul weiter, damit die Authentifizierung erfolgt.

Abbildung 11-1 zeigt ein einfaches Beispiel, wie ESX Server 3 Übertragungen vom VI-Client authentifiziert.

Abbildung 11-1. Authentifizierung für VI Client-Datenverkehr mit ESX Server 3



ESX Server-Authentifizierungstransaktionen mit VI Web Access und Netzwerkverwaltungsclients anderer Anbieter ähneln direkten Interaktionen mit dem Prozess `vmware-hostd`.

Damit die Authentifizierung an Ihrem Standort effizient funktioniert, müssen Sie gegebenenfalls grundlegende Aufgaben wie die Einrichtung von Benutzern, Gruppen, Berechtigungen und Rollen vornehmen, die Benutzerattribute konfigurieren, eigene Zertifikate erstellen, ggf. SSL einrichten usw.

Informationen zu Benutzern, Gruppen, Berechtigungen und Rollen

Der Zugriff auf einen ESX Server-Host und dessen Ressourcen wird dann gewährt, wenn sich ein bekannter Benutzer mit den entsprechenden Berechtigungen auf dem Host mit einem Kennwort anmeldet, das dem für den Benutzer gespeicherten Kennwort entspricht. VirtualCenter verwendet ein ähnliches Verfahren, um Benutzern Zugriff zu gewähren. VirtualCenter- und ESX Server geben mithilfe von den Benutzern zugewiesenen Berechtigungen an, worauf die Benutzer zugreifen dürfen. So kann zum Beispiel ein Benutzer die Berechtigung haben, virtuelle Maschinen auf einem Host zu erstellen, während ein anderer Benutzer zwar die Berechtigung hat, virtuelle Maschinen hochzufahren, nicht jedoch, sie zu erstellen.

Anhand der Kombination aus Benutzername, Kennwort und Berechtigungen authentifizieren VirtualCenter und ESX Server 3-Hosts einen Benutzer für den Zugriff und autorisieren den Benutzer zum Durchführen von Aktivitäten. Dazu unterhalten VirtualCenter und der ESX Server-Hosts Listen autorisierter Benutzer mit ihren Kennwörtern und den ihnen zugewiesenen Berechtigungen. VirtualCenter und ESX Server-Hosts verweigern den Zugriff unter folgenden Umständen:

- Ein Benutzer, der nicht in der Benutzerliste aufgeführt wird, versucht sich anzumelden.
- Ein Benutzer gibt ein falsches Kennwort ein.
- Ein Benutzer ist zwar im Verzeichnis aufgeführt, hat aber keine Berechtigungen.
- Ein Benutzer, der sich erfolgreich angemeldet hat, versucht Vorgänge auszuführen, für die er keine Berechtigung besitzt.

Zur Verwaltung von ESX Server-Hosts und VirtualCenter gehört auch die Entwicklung von Benutzer- und Berechtigungsmodellen, d. h. Grundplänen zur Behandlung bestimmter Benutzerarten und zur Zuweisung der Berechtigungen. Beachten Sie bei der Entwicklung von Benutzer- und Berechtigungsmodellen Folgendes:

- ESX Server 3 und VirtualCenter verwenden Privilegiengruppen, sog. *Rollen*, um zu steuern, welche Vorgänge bestimmte Benutzer oder Gruppen ausführen dürfen. ESX Server 3 und VirtualCenter bieten verschiedene vordefinierte Rollen. Sie können jedoch auch eigene neue Rollen erstellen.
- Sie können Benutzer leichter verwalten, wenn Sie sie Gruppen zuordnen. Wenn Sie Gruppen erstellen, können Sie eine Rolle auf die Gruppe anwenden, und diese Rolle wird von allen Benutzern in der Gruppe übernommen.

Grundlegendes zu Benutzern

Ein Benutzer ist eine Person, die sich am ESX Server 3-Host oder an VirtualCenter anmelden darf. ESX Server 3-Benutzer werden in zwei Kategorien unterteilt: Benutzer, die über VirtualCenter auf den ESX Server 3-Host zugreifen, und Benutzer, die direkt auf den ESX Server 3-Host zugreifen, indem Sie sich über den VI-Client, VI Web Access, Clients von Drittanbietern oder eine Befehlsshell anmelden. Die Benutzer in diesen beiden Kategorien haben folgenden Hintergrund.

- **VirtualCenter-Benutzer** – Autorisierte Benutzer für VirtualCenter sind die Benutzer, die in der Windows-Domänenliste von VirtualCenter aufgeführt sind, oder lokale Windows-Benutzer auf dem VirtualCenter-Host.

  In VirtualCenter können Sie Benutzer nicht erstellen, entfernen oder anderweitig ändern. Um das Benutzerverzeichnis oder Benutzerkennwörter zu ändern, müssen Sie die Programme verwenden, mit denen Sie die Windows-Domäne verwalten.

  Alle Änderungen, die Sie an der Windows-Domäne vornehmen, werden von VirtualCenter übernommen. Da Sie jedoch die Benutzer nicht direkt in VirtualCenter verwalten können, enthält die Benutzeroberfläche auch kein Benutzerverzeichnis, das angezeigt werden kann. Nur bei der Auswahl von Benutzern und Gruppen während der Rollenzuweisung stehen Benutzer- und Gruppenverzeichnisse zur Verfügung. Die Änderungen werden nur sichtbar, wenn Sie Benutzer zum Konfigurieren von Berechtigungen auswählen.

- **Benutzer mit direktem Zugriff** – Benutzer, die zum direkten Arbeiten auf einem ESX Server 3-Host autorisiert sind, werden der internen Benutzerliste standardmäßig bei der Installation oder nach der Installation von einem Systemadministrator hinzugefügt.

  Wenn Sie sich auf dem Host als Administrator anmelden, können Sie verschiedene Management-Aktivitäten für diese Benutzer ausführen, z. B. Kennwörter, Gruppenmitgliedschaft, Berechtigungen usw. ändern. Außerdem können Sie Benutzer hinzufügen und entfernen.

Die von VirtualCenter geführte Benutzerliste ist eine grundlegend andere als die Benutzerliste des ESX Server 3-Hosts. Selbst wenn die Benutzerlisten von Host und VirtualCenter die gleichen Benutzer zu haben scheinen (zum Beispiel einen Benutzer mit dem Namen *devuser*), sollten diese Benutzer als verschiedene Benutzer behandelt werden, die zufällig den gleichen Namen haben. Die Attribute von „devuser“ in VirtualCenter wie Berechtigungen, Kennwörter usw. sind von den Attributen von „devuser“ auf dem ESX Server 3-Host getrennt. Wenn Sie sich an VirtualCenter als „devuser“ anmelden, können Sie z. B. über die Berechtigung verfügen, Dateien aus einem Datenspeicher anzusehen und zu löschen, was nicht der Fall sein muss, wenn Sie sich auf dem ESX Server 3-Host als „devuser“ anmelden.

Aufgrund der Verwirrung, die doppelte Namen stiften können, empfiehlt VMware, dass Sie vor der Erstellung von ESX Server 3-Host-Benutzern das Benutzerverzeichnis von VirtualCenter überprüfen, um doppelte Namen zu vermeiden. Das Verzeichnis der VirtualCenter-Benutzer finden Sie im Windows-Domänenverzeichnis.

Grundlegendes zu Gruppen

Bestimmte Benutzerattribute können Sie effektiver verwalten, indem Sie Gruppen erstellen. Eine Gruppe ist eine Zusammenstellung von Benutzern, die durch gemeinsame Regeln und Berechtigungen verwaltet werden sollen. Wenn Sie einer Gruppe Berechtigungen zuweisen, werden diese von allen Benutzern in der Gruppe übernommen, wodurch Sie die Benutzerprofile nicht einzeln bearbeiten müssen. Daher kann die Verwendung von Gruppen die Zeit zur Implementierung des Berechtigungsmodells wesentlich verkürzen und künftig die Skalierbarkeit verbessern.

Als Administrator müssen Sie entscheiden, wie die Gruppen strukturiert werden sollen, um die Sicherheits- und Verwendungsziele zu erreichen. Sie haben zum Beispiel drei Teilzeitkräfte in der Vertriebsabteilung, die an verschiedenen Tagen arbeiten und zwar auf eine bestimmte virtuelle Maschine zugreifen sollen, nicht jedoch auf die virtuellen Maschinen des Vertriebsleiters. In diesem Fall können Sie eine Gruppe, z. B. *VertriebTeilzeit* einrichten, zu der diese drei Teilzeitkräfte gehören: Maria, Thomas und Peter. Sie können dann der Gruppe „VertriebTeilzeit“ die Berechtigung zur Interaktion mit nur einem Objekt, der Virtuellen Maschine A, zuweisen. Maria, Thomas und Peter übernehmen diese Berechtigungen und können die Virtuelle Maschine A hochfahren, Konsolensitzungen auf der Virtuellen Maschine A aufrufen usw. Sie können diese Vorgänge jedoch nicht auf den virtuellen Maschinen des Vertriebsleiters durchführen: den virtuellen Maschinen B, C und D.

Die Gruppenverzeichnisse in VirtualCenter und auf dem ESX Server 3-Host stammen aus den gleichen Quellen wie die entsprechenden Benutzerverzeichnisse. Wenn Sie mit VirtualCenter arbeiten, wird das Gruppenverzeichnis von der Windows-Domäne abgerufen. Wenn Sie direkt an einem ESX Server 3-Host angemeldet sind, wird die Liste der Benutzergruppen aus einer Tabelle aufgerufen, die vom Host verwaltet wird. Die Empfehlungen zur Behandlung von Gruppenverzeichnissen entsprechen den Empfehlungen für Benutzerverzeichnisse.

Grundlegendes zu Berechtigungen

Für ESX Server 3 und VirtualCenter werden Berechtigungen als Zugriffsrollen definiert, die aus einem Benutzer und der dem Benutzer zugewiesenen Rolle für ein Objekt wie z. B. einer virtuellen Maschine oder einem ESX Server 3-Host bestehen. Berechtigungen geben Benutzern das Recht, bestimmte Vorgänge auszuführen und bestimmte Objekte auf einem ESX Server 3-Host oder, wenn Benutzer von VirtualCenter aus arbeiten, alle von VirtualCenter verwalteten Objekte zu verwalten. Wenn Sie zum Beispiel Speicher für einen ESX Server 3-Host konfigurieren möchten, müssen Sie über eine Berechtigung zur Hostkonfiguration verfügen.

Die meisten VirtualCenter- und ESX Server 3-Benutzer können Objekte des Hosts nur in eingeschränktem Maße ändern. Benutzer mit der Rolle **Administrator** haben jedoch Vollzugriff auf alle virtuellen Objekte wie Datenspeicher, Hosts, virtuelle Maschinen und Ressourcenpools. Die Rolle **Administrator** wird standardmäßig dem Root-Benutzer gewährt. Wenn VirtualCenter den Host verwaltet, hat **vpxuser** auch Administratorrechte. Administratoren haben die folgenden Berechtigungen:

- **root** – Der Root-Benutzer kann auf dem ESX Server 3-Host, an dem er sich angemeldet hat, alle Steuerungsvorgänge wie z. B. die Verwaltung von Berechtigungen, die Erstellung von Gruppen und Benutzern, die Ereignisverwaltung usw. vornehmen. Ein Root-Benutzer, der auf einem ESX Server 3-Host angemeldet ist, kann jedoch die Aktivitäten anderer Hosts in der übergeordneten ESX Server 3-Bereitstellung nicht beeinflussen.

  Aus Sicherheitsgründen sollten Sie dem Root-Benutzer nicht die Rolle **Administrator** gewähren. In diesem Fall können Sie die Berechtigungen nach der Installation so ändern, dass der Root-Benutzer keine weiteren Administratorrechte hat, oder Sie löschen alle Zugriffsrechte des Root-Benutzers über den VI-Client, wie im Kapitel „Verwalten von Benutzern, Gruppen, Berechtigungen und Rollen" von *Grundlagen der Systemverwaltung* beschrieben. Wenn Sie dies tun, müssen Sie auf der Root-Ebene zunächst eine andere Genehmigung erteilen, die ein anderer Benutzer mit der Rolle des Administrators erhält.

  Die Zuweisung der Administratorenrolle auf verschiedene Benutzer gewährleistet die Nachvollziehbarkeit und somit die Sicherheit. Der VI-Client protokolliert alle Aktionen des Administrators als Ereignisse und gibt ein Überwachungsprotokoll aus. Sie können diese Funktion zur Verbesserung der Verantwortlichkeit der verschiedenen Benutzer verwenden, die für einen Host als Administrator fungieren. Wenn alle Administratoren sich am Host als Root-Benutzer anmelden, können Sie nicht wissen, welcher Administrator eine Aktion ausgeführt hat. Wenn Sie jedoch mehrere Berechtigungen auf Root-Ebene anlegen, die jeweils einem anderen Benutzer oder einer anderen Benutzergruppe zugewiesen sind, können Sie die Aktionen jedes Administrators oder jeder Administratorengruppe gut nachvollziehen.

  Nachdem Sie einen alternativen Administrator-Benutzer angelegt haben, können Sie sicher die Berechtigungen des Root-Benutzers löschen oder dessen Rolle in der Form ändern, dass seine Rechte begrenzt werden. Wenn Sie die Berechtigungen des Root-Benutzers löschen oder ändern, müssen Sie den neu erstellten Benutzer als Ausgangspunkt für die Hostauthentifizierung verwenden, sobald der Host von Ihnen unter die Verwaltung von VirtualCenter gestellt wird. Siehe „Grundlegendes zu Rollen" auf Seite 228.

HINWEIS Konfigurationsbefehle, die Sie über die Befehlszeilenoberfläche ausführen (`esxcfg`-Befehle), führen keine Zugriffsprüfung durch. Selbst wenn Sie die Berechtigungen des Root-Benutzers einschränken, wirkt sich dies nicht auf die Befehle aus, die er über die Befehlszeilenschnittstelle ausführen kann.

- **vpxuser** – Dieser Benutzer ist VirtualCenter, das mit Administratorrechten auf dem ESX Server 3-Host agiert, wodurch es Vorgänge für diesen verwalten kann. **vpxuser** wird erstellt, wenn der ESX Server 3-Host an VirtualCenter angebunden wird. Diesen Benutzer gibt es auf dem ESX Server 3-Host nur, wenn der Host über VirtualCenter verwaltet wird.

  Wenn ein ESX Server 3-Host über VirtualCenter verwaltet wird, hat VirtualCenter Administratorrechte auf diesem Host. So kann VirtualCenter zum Beispiel virtuelle Maschinen auf Hosts verschieben und Konfigurationsänderungen vornehmen, die für die Unterstützung virtueller Maschinen notwendig sind.

  Der Administrator von VirtualCenter kann über **vpxuser** viele der Aufgaben des Root-Benutzers auf dem Host durchführen und Aufgaben planen, Vorlagen erstellen und nutzen usw. Es gibt jedoch bestimmte Vorgänge, die Sie als VirtualCenter-Administrator nicht ausführen können. Diese Aktivitäten, zu denen die direkte Erstellung, Löschung oder Bearbeitung von Benutzern und Gruppen für ESX Server 3-Hosts gehören, können nur von einem Benutzer mit Administratorrechten direkt auf dem entsprechenden ESX Server 3-Host vorgenommen werden.

VORSICHT Ändern Sie **vpxuser** und die dazugehörigen Berechtigungen nicht. Ansonsten kann es zu Problemen bei der Verwaltung des ESX Server-Hosts über VirtualCenter kommen.

Wenn Sie die Rolle **Administrator** auf einem ESX Server 3i-Host haben, können Sie einzelnen Benutzern und Gruppen auf diesem Host Berechtigungen zuweisen. Wenn Sie als Administrator an VirtualCenter angemeldet sind, können Sie allen Benutzern oder Gruppen im von VirtualCenter übernommenen Windows-Domänenverzeichnis Berechtigungen zuweisen.

VirtualCenter registriert alle ausgewählten Benutzer oder Gruppen der Windows-Domäne durch den Prozess der Zuweisung von Berechtigungen. Standardmäßig werden allen Benutzern, die zur lokalen Gruppe **Windows-Administratoren (Windows Administrators)** auf dem VirtualCenter Server gehören, die gleichen Zugriffsrechte wie Benutzern mit der Rolle **Administrator** zugewiesen. Benutzer, die Mitglieder der Gruppe **Administratoren (Administrators)** sind, können sich anmelden und verfügen dann über Vollzugriff.

Aus Sicherheitsgründen sollten Sie die Gruppe **Windows-Administratoren (Windows Administrators)** aus der Rolle **Administrator** entfernen. Sie können Berechtigungen nach der Installation so ändern, dass die Gruppe **Windows-Administratoren (Windows Administrators)** nicht über Administratorrechte verfügt. Sie können auch im VI-Client die Berechtigungen der Gruppe **Windows-Administratoren (Windows Administrators)** löschen. Wenn Sie dies tun, müssen Sie auf der Root-Ebene zunächst eine andere Berechtigung einrichten, bei der ein anderer Benutzer der Rolle **Administrator** zugewiesen ist.

Das Verfahren zur Konfiguration von Berechtigungen direkt auf einem ESX Server 3i-Host entspricht dem Verfahren zur Konfiguration von Berechtigungen in VirtualCenter. Auch die Liste der Berechtigungen ist für ESX Server 3i und in VirtualCenter gleich.

Weitere Informationen zur Konfiguration von Berechtigungen und zu den Rechten, die zugewiesen werden können, finden Sie in *Grundlagen der Systemverwaltung*.

Grundlegendes zu Rollen

VirtualCenter und ESX Server gewähren nur Benutzern Zugriff auf Objekte, denen Berechtigungen für das jeweilige Objekt zugewiesen wurden. Wenn Sie einem Benutzer oder einer Benutzergruppe Berechtigungen für das Objekt zuweisen, fassen Sie den Benutzer oder die Gruppe mit einer Rolle zu einem Paar zusammen. Bei einer Rolle handelt es sich um einen vordefinierten Satz von Berechtigungen.

Für ESX Server-Hosts gibt es drei Standardrollen. Es ist nicht möglich, die Berechtigungen für diese drei Rollen zu ändern. Jede nachfolgende Standardrolle enthält die Berechtigungen der vorhergehenden Rolle. So übernimmt beispielsweise die Rolle **Administrator** die Rechte der Rolle **Nur lesen (Read Only)**. Rollen, die Sie selbst anlegen, übernehmen keine Berechtigungen von den Standardrollen. Es gibt folgende Standardrollen:

- **Kein Zugriff** – Benutzer, denen diese Rolle für ein bestimmtes Objekt zugewiesen wurde, können das Objekt weder anzeigen noch ändern. So kann zum Beispiel ein Benutzer, dem für eine bestimmte virtuelle Maschine die Rolle **Kein Zugriff (No Access)** zugewiesen wurde, die virtuelle Maschine nicht in der VI-Client-Bestandsliste sehen, wenn er sich am ESX Server-Host anmeldet. Wenn einem Benutzer für ein bestimmtes Objekt diese Rolle zugewiesen wurde, kann er die Registerkarten im VI-Client für das gesperrte Objekt auswählen, auf der jedoch kein Inhalt angezeigt wird. Wenn der Benutzer zum Beispiel keinen Zugriff auf virtuelle Maschinen hat, kann er auf die Registerkarte **Virtuelle Maschinen (Virtual Machines)** klicken, aber ihm werden weder das Verzeichnis der virtuellen Maschinen auf der Registerkarte noch die Statusinformationen angezeigt. Die Tabelle ist leer.

Die Rolle **Kein Zugriff (No Access)** ist die Standardrolle, die allen Benutzern oder Gruppen, die Sie auf einem ESX Server 3-Host erstellen, zugewiesen wird. Sie können die Rolle neuer Benutzer oder Gruppen objektabhängig mit höheren oder niedrigeren Berechtigungen ausstatten.

Die einzigen Benutzer, denen die Rolle **Kein Zugriff (No Access)** nicht standardmäßig zugewiesen wird, sind der Root-Benutzer und **vpxuser**. Stattdessen wird ihnen die Rolle **Administrator** zugewiesen.

Sie können die Berechtigungen des Root-Benutzers insgesamt löschen oder seine Rolle auf **Kein Zugriff (No Access)** festlegen, sofern Sie zunächst auf Root-Ebene eine Ersatzberechtigung mit der Rolle **Administrator** anlegen und diese Rolle einem anderen Benutzer zuweisen. Wenn Sie die Berechtigungen des Root-Benutzers löschen oder ändern, müssen Sie den neu erstellten Benutzer als Ausgangspunkt für die Hostauthentifizierung verwenden, wenn Sie den Host unter die Verwaltung von VirtualCenter stellen.

- **Nur Lesen** – Benutzer, denen diese Rolle für ein Objekt zugewiesen wurde, können den Status des Objekts und Details zum Objekt anzeigen.

  Mit dieser Rolle kann ein Benutzer die virtuelle Maschine, den Host und die Ressourcenpoolattribute anzeigen. Der Benutzer kann jedoch nicht die Remotekonsole eines Hosts anzeigen. Alle Vorgänge über die Menüs und Symbolleisten sind nicht zugelassen.

- **Administrator** – Benutzer, denen diese Rolle für ein Objekt zugewiesen wurde, können sämtliche Vorgänge auf ein Objekt anwenden und diese anzeigen. Zu dieser Rolle gehören alle Berechtigungen, über die auch die Rolle **Nur Lesen (Read Only)** verfügt.

Benutzerdefinierte Rollen können Sie mit den Rollenbearbeitungsdienstprogrammen auf dem VI-Client erstellen und an Ihre Anforderungen anpassen. Wenn Sie den mit VirtualCenter verbundenen VI-Client zur Verwaltung der ESX Server 3-Hosts verwenden, stehen Ihnen in VirtualCenter zusätzliche Rollen zur Auswahl. Auf die Rollen, die Sie direkt auf einem ESX Server 3-Host erstellen, kann nicht innerhalb von VirtualCenter zugegriffen werden. Sie können diese Rollen nur verwenden, wenn Sie sich direkt über den VI-Client am Host anmelden.

Wenn Sie ESX Server 3-Hosts über VirtualCenter verwalten, beachten Sie, dass die Verwendung benutzerdefinierter Rollen auf dem Host und in VirtualCenter zu Verwirrung und Missbrauch führen kann. Bei dieser Art der Konfiguration empfiehlt VMware, benutzerdefinierte Rollen nur in VirtualCenter zu verwenden. Informationen zum Erstellen, Ändern und Löschen von Rollen sowie zu den zusätzlich in VirtualCenter verfügbaren Rollen finden Sie in *Grundlagen der Systemverwaltung*.

Verwalten von Benutzern und Gruppen auf ESX Server 3-Hosts

Wenn Sie direkt über den VI-Client mit einem ESX Server 3-Host verbunden sind, können Sie Benutzer und Gruppen erstellen, bearbeiten und löschen. Diese Benutzer und Gruppen werden im VI-Client angezeigt, wenn Sie sich am ESX Server 3-Host anmelden. Bei Anmeldung an VirtualCenter stehen sie jedoch nicht zur Verfügung.

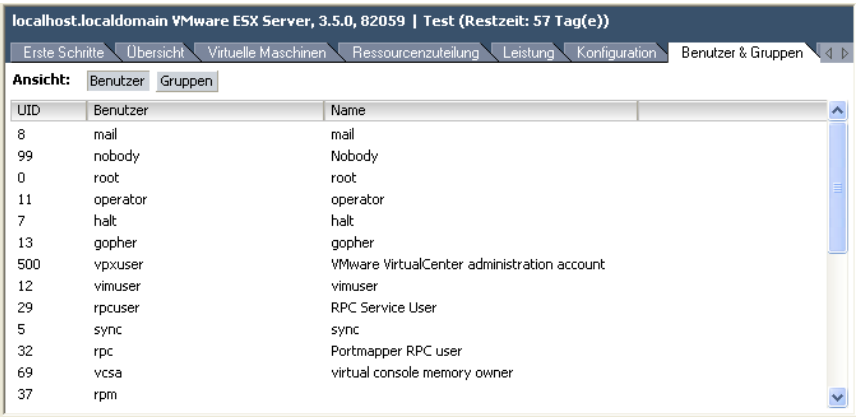
Anzeigen und Exportieren von Benutzer- und Gruppeninformationen

Benutzer und Gruppen werden über die Registerkarte **Benutzer und Gruppen (Users & Groups)** im VI-Client verwaltet. Diese Registerkarte zeigt die Tabelle **Benutzer (Users)** oder **Gruppen (Groups)** an, je nachdem, ob Sie auf die Schaltfläche **Benutzer (Users)** oder **Gruppen (Groups)** klicken.

Sie können auch über eine direkte Verbindung mit dem ESX Server 3-Host Rollen erstellen und Berechtigungen festlegen. Da diese Aufgaben jedoch häufiger in VirtualCenter durchgeführt werden, lesen Sie die Abschnitte in *Grundlagen der Systemverwaltung*, um Informationen zum Verwalten von Berechtigungen und Rollen zu erhalten.

Abbildung 11-2 zeigt die Tabelle **Benutzer (Users)**. Die Tabelle **Gruppen (Groups)** sieht ähnlich aus.

Abbildung 11-2. Tabelle „Benutzer“



UID	Benutzer	Name
8	mail	mail
99	nobody	Nobody
0	root	root
11	operator	operator
7	halt	halt
13	gopher	gopher
500	vpxuser	VMware VirtualCenter administration account
12	vimuser	vimuser
29	rpcuser	RPC Service User
5	sync	sync
32	rpc	Portmapper RPC user
69	vcsa	virtual console memory owner
37	rpm	

Sie können die Listen nach Spalten sortieren, Spalten ein- oder ausblenden und die Listen in Formate exportieren, die Sie zur Erstellung von Berichten oder zur Veröffentlichung von Benutzer- oder Gruppenverzeichnissen im Internet verwenden können.

So werden ESX Server 3-Benutzer oder -Gruppen angezeigt und sortiert

1 Melden Sie sich über den ESX Server 3-Host am VI-Client an.

2 Wählen Sie den Server in der Bestandsliste aus.

3 Klicken Sie auf die Registerkarte **Benutzer und Gruppen (Users & Groups)** und dann auf **Benutzer (Users)** oder **Gruppen (Groups)**.

4 Führen Sie je nach Bedarf folgende Schritte aus:

- Wenn Sie die Tabelle nach einer Spalte sortieren möchten, klicken Sie auf die entsprechende Spaltenüberschrift.
- Wenn Sie eine Spalte ein- oder ausblenden möchten, klicken Sie mit der rechten Maustaste auf eine der Spaltenüberschriften, und aktivieren oder deaktivieren Sie den Namen der Spalte, die Sie ein- oder ausblenden möchten.

So exportieren Sie Daten aus der ESX Server 3-Tabelle „Benutzer“ oder „Gruppen“

1 Melden Sie sich über den ESX Server 3-Host am VI-Client an.

2 Wählen Sie den Server in der Bestandsliste aus.

3 Klicken Sie auf die Registerkarte **Benutzer und Gruppen (Users & Groups)** und dann auf **Benutzer (Users)** oder **Gruppen (Groups)**.

4 Legen Sie die Sortierreihenfolge der Tabelle fest, und blenden Sie Spalten ein oder aus, je nachdem welche Daten in der Exportdatei enthalten sein sollen.

5 Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle in der Tabelle **Benutzer**, und klicken Sie auf **Exportieren (Export)**. Das Dialogfeld **Speichern unter (Save As)** wird angezeigt.

6 Wählen Sie einen Pfad, geben Sie einen Dateinamen ein, und wählen Sie den Dateityp aus.

7 Klicken Sie auf **OK**.

Verwalten der Tabelle „Benutzer“

Sie können Benutzer zur Tabelle **Benutzer (Users)** eines ESX Server 3-Hosts hinzufügen, Benutzer entfernen und andere Benutzerattribute wie Kennwort und Gruppenmitgliedschaft ändern. Durch diese Aktivitäten ändern Sie die interne, vom ESX Server 3-Host verwaltete Benutzerliste.

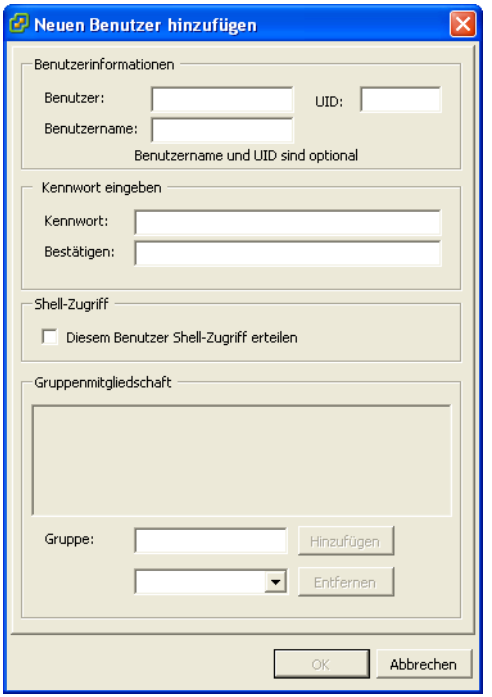
So fügen Sie einen Benutzer der ESX Server 3-Tabelle „Benutzer“ hinzu

1 Melden Sie sich über den ESX Server 3-Host am VI-Client an.

2 Wählen Sie den Server in der Bestandsliste aus.

3 Klicken Sie auf die Registerkarte **Benutzer und Gruppen (Users & Groups)** und dann auf **Benutzer (Users)**.

4 Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle der Tabelle **Benutzer (Users)**, und klicken Sie auf **Hinzufügen (Add)**. Das Dialogfeld **Neuen Benutzer hinzufügen (Add New User)** wird angezeigt.



5 Geben Sie eine Anmeldung, einen Benutzernamen, eine numerische Benutzer-ID und ein Kennwort ein.

Die Angabe des Benutzernamens und der ID sind optional. Wenn Sie keine Benutzer-ID angeben, weist der VI-Client die nächste verfügbare Benutzer-ID zu.

Das Kennwort muss hinsichtlich Länge und Komplexität den Anforderungen im Abschnitt „Kennwortbeschränkungen“ auf Seite 254 entsprechen. Der ESX Server 3-Host prüft nur dann die Einhaltung der Kennwortrichtlinien, wenn Sie zu Authentifizierungszwecken zum Plug-In `pam_passwdqc.so` gewechselt sind. Die Kennworteinstellungen im Standardauthentifizierungs-Plug-In `pam_cracklib.so` werden nicht erzwungen.

6 Wenn der Benutzer in der Lage sein soll, über eine Befehlsshell auf den ESX Server 3-Host zuzugreifen, aktivieren Sie das Kontrollkästchen **Diesem Benutzer Shell-Zugriff erteilen (Grant shell access to this user)**.

Im Allgemeinen sollte der Shellzugriff nur ESX Server 3-Host-Benutzern erteilt werden, die diesen Zugriff auf den Host über eine Shell statt über den VI-Client tatsächlich benötigen. Benutzer, die nur über den VI-Client auf den Host zugreifen, benötigen keinen Shellzugriff.

7 Geben Sie die Gruppennamen der Gruppen ein, zu denen der Benutzer gehören soll, und klicken Sie auf **Hinzufügen (Add)**.

Wenn Sie einen nicht vorhandenen Gruppennamen eingeben, gibt der VI-Client eine Warnmeldung aus und fügt die Gruppe nicht der Liste **Gruppenmitgliedschaft (Group membership)** hinzu.

8 Klicken Sie auf **OK**.

Der Anmeldungs- und Benutzername, den Sie eingegeben haben, wird jetzt in der Tabelle **Benutzer (Users)** angezeigt.

So ändern Sie die Einstellungen für einen Benutzer

1 Melden Sie sich über den ESX Server 3-Host am VI-Client an.

2 Wählen Sie den Server in der Bestandsliste aus.

3 Klicken Sie auf die Registerkarte **Benutzer und Gruppen (Users & Groups)** und dann auf **Benutzer (Users)**.

4 Klicken Sie mit der rechten Maustaste auf den zu ändernden Benutzer und dann auf **Bearbeiten (Edit)**, um das Dialogfeld **Benutzer bearbeiten (Edit User)** zu öffnen.

5 Wenn Sie die UID ändern möchten, geben Sie im Feld **Benutzer (UID)** eine numerische UID ein.

Der VI Client weist einem Benutzer bei seiner Erstellung die UID zu. In den meisten Fällen muss diese Zuweisung nicht geändert werden.

6 Geben Sie einen neuen Benutzernamen ein.

7 Wenn Sie das Kennwort eines Benutzers ändern möchten, aktivieren Sie das Kontrollkästchen **Kennwort ändern (Change Password)**, und geben Sie ein neues Kennwort ein.

   Das Kennwort muss hinsichtlich Länge und Komplexität den Anforderungen im Abschnitt „Kennwortbeschränkungen“ auf Seite 254 entsprechen. Der ESX Server 3-Host prüft nur dann die Einhaltung der Kennwortrichtlinien, wenn Sie zu Authentifizierungszwecken zum Plug-In `pam_passwdqc.so` gewechselt sind. Die Kennworteinstellungen im Standardauthentifizierungs-Plug-In `pam_cracklib.so` werden nicht erzwungen.

8 Um die Einstellung zu ändern, dass Benutzer über eine Befehlsshell auf den ESX Server 3-Host zugreifen können, aktivieren oder deaktivieren Sie das Kontrollkästchen **Diesem Benutzer Shell-Zugriff erteilen (Grant shell access to this user)**.

9 Wenn Sie den Benutzer einer anderen Gruppe hinzufügen möchten, geben Sie den Gruppennamen ein, und klicken Sie auf **Hinzufügen (Add)**.

   Wenn Sie einen nicht vorhandenen Gruppennamen eingeben, gibt der VI-Client eine Warnmeldung aus und fügt die Gruppe nicht der Liste **Gruppenmitgliedschaft (Group membership)** hinzu.

10 Zum Entfernen des Benutzers wählen Sie den Gruppennamen in der Liste aus und klicken auf **Entfernen (Remove)**.

11 Klicken Sie auf **OK**.

So entfernen Sie einen Benutzer aus der ESX Server 3-Tabelle „Benutzer“

1 Melden Sie sich über den ESX Server-Host 3 am VI-Client an.

2 Wählen Sie den Server in der Bestandsliste aus.

3 Klicken Sie auf die Registerkarte **Benutzer und Gruppen (Users & Groups)** und dann auf **Benutzer (Users)**.

4 Klicken Sie mit der rechten Maustaste auf den Benutzer, den Sie entfernen möchten, und klicken Sie auf **Entfernen (Remove)**.

VORSICHT Entfernen Sie *nicht* den Root-Benutzer.

Verwalten der Tabelle „Gruppen“

Sie können Gruppen der Tabelle **Gruppen (Groups)** eines ESX Server 3-Hosts hinzufügen, Gruppen entfernen oder Gruppenmitglieder hinzufügen oder entfernen. Durch diese Aktivitäten ändern Sie die interne, vom ESX Server 3-Host verwaltete Gruppenliste.

So fügen Sie eine Gruppe der ESX Server 3-Tabelle „Gruppe“ hinzu

1 Melden Sie sich über den ESX Server 3-Host am VI-Client an.

2 Wählen Sie den Server in der Bestandsliste aus.

3 Klicken Sie auf die Registerkarte **Benutzer und Gruppen (Users & Groups)** und dann auf **Gruppen (Groups)**.

4 Klicken Sie mit der rechten Maustaste auf eine beliebige Stelle der Tabelle **Gruppen (Groups)** und dann auf **Hinzufügen (Add)**. Das Dialogfeld **Neue Gruppe erstellen (Create New Group)** wird angezeigt.

5 Geben Sie einen Gruppennamen und in das Feld **Gruppen-ID (Group ID)** eine numerische Gruppen-ID (GID) ein.

   Die Angabe der GID ist nicht zwingend erforderlich. Wenn Sie keine GID angeben, weist der VI-Client die nächste verfügbare Gruppen-ID zu.

6 Geben Sie die Benutzernamen aller Benutzer ein, die zur Gruppe gehören sollen, und klicken Sie auf **Hinzufügen (Add)**.

   Wenn Sie einen nicht vorhandenen Benutzernamen eingeben, gibt der VI-Client eine Warnmeldung aus und fügt den Benutzer nicht zum Verzeichnis **Benutzer in dieser Gruppe (Users in this group)** hinzu.

7 Klicken Sie auf **OK**.

Die Gruppen-ID und der Gruppenname, den Sie eingegeben haben, werden jetzt in der Tabelle **Gruppen (Groups)** angezeigt.

So werden Benutzer einer Gruppe hinzugefügt oder aus dieser entfernt

1 Melden Sie sich über den ESX Server 3-Host am VI-Client an.

2 Wählen Sie den Server in der Bestandsliste aus.

3 Klicken Sie auf die Registerkarte **Benutzer und Gruppen (Users & Groups)** und dann auf **Gruppen (Groups)**.

4 Klicken Sie mit der rechten Maustaste auf die zu ändernde Gruppe und dann auf **Bearbeiten (Edit)**, um das Dialogfeld **Gruppe bearbeiten (Edit Group)** zu öffnen.

5 Zum Hinzufügen eines Benutzers zu dieser Gruppe geben Sie den Benutzernamen ein und klicken auf **Hinzufügen (Add)**.

Wenn Sie einen nicht vorhandenen Benutzernamen eingeben, gibt der VI-Client eine Warnmeldung aus und fügt den Benutzer nicht zum Verzeichnis **Benutzer in dieser Gruppe (Users in this group)** hinzu.

6 Wenn Sie einen Benutzer aus der Gruppe entfernen möchten, wählen Sie den Benutzernamen aus dem Verzeichnis aus und klicken Sie auf **Entfernen (Remove)**.

7 Klicken Sie auf **OK**.

So entfernen Sie eine Gruppe aus der ESX Server 3-Tabelle „Gruppen“

1 Melden Sie sich über den ESX Server 3-Host am VI-Client an.

2 Wählen Sie den Server in der Bestandsliste aus.

3 Klicken Sie auf die Registerkarte **Benutzer und Gruppen (Users & Groups)** und dann auf **Gruppen (Groups)**.

4 Klicken Sie mit der rechten Maustaste auf die Gruppe, die Sie entfernen möchten, und klicken Sie auf **Entfernen (Remove)**.

VORSICHT Entfernen Sie *nicht* den Root-Benutzer.

Verschlüsselungs- und Sicherheitszertifikate für ESX Server 3

ESX Server unterstützt SSL Version 3, und TLS Version 1, die anschließend als SSL (Secure Socket Layer) bezeichnet werden. SSL dient der Absicherung von Datenübertragungen. Ist SSL aktiviert, bleiben Daten so vertraulich, dass sie nicht gelesen, und so geschützt, dass sie nicht unbemerkt während der Übertragung geändert werden können. Sämtlicher Netzwerkdatenverkehr wird verschlüsselt, solange die folgenden Bedingungen gelten:

- Der Web-Proxy-Dienst wurde nicht so geändert, dass er unverschlüsselten Datenverkehr für den Port durchlässt.
- Bei der Firewall der Servicekonsole wurde die mittlere oder hohe Sicherheit eingestellt. Informationen zur Konfiguration der Firewall der Servicekonsole finden Sie unter „Konfiguration der Servicekonsolen-Firewall“ auf Seite 249.

SSL ist nicht standardmäßig aktiviert, sodass der Netzwerkdatenverkehr erst verschlüsselt wird, nachdem Sie diese Funktion aktiviert haben. SSL schützt die einleitende Verbindung zwischen VI-Clients und VirtualCenter. Nachfolgende Datenübertragungen werden nicht verschlüsselt. Um die von Zertifikaten in ESX Server 3 gebotene Sicherheit vollständig zu aktivieren, müssen Sie die Zertifikatsprüfung aktivieren und neue Zertifikate installieren.

So aktivieren Sie die Zertifikatsprüfung

1 Melden Sie sich über den VI-Client an einem VirtualCenter-Server an.

2 Klicken Sie auf **Verwaltung (Administration)** > **VirtualCenter Managementserver – Konfiguration (Virtual Center Management Server Configuration)**.

   Das Dialogfeld **VirtualCenter Managementserver – Konfiguration (Virtual Center Management Server Configuration)** wird angezeigt.

3 Klicken Sie im linken Bereich auf **SSL-Einstellungen (SSL Settings)**, und aktivieren Sie das Kontrollkästchen **Hostzertifikate prüfen (Check host certificates)**.

4 Klicken Sie auf **OK**.

Um die Vorteile der Zertifikatsprüfung voll nutzen zu können, müssen Sie neue Zertifikate installieren. Die Anfangszertifikate werden von ESX Server erstellt und auf dem Host gespeichert. Die Zertifikate, die zur Absicherung von VirtualCenter- und VI Web Access-Sitzungen verwendet werden, wurden nicht von einer vertrauenswürdigen Zertifizierungsstelle signiert und bieten daher nicht die Authentifizierungssicherheit, die in einer Produktionsumgebung notwendig sein kann. So sind beispielsweise selbst signierte Zertifikate anfällig für Man-in-the-Middle-Angriffe. Wenn Sie verschlüsselte Remoteverbindungen extern verwenden möchten, kann es ggf. sinnvoll sein, ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle zu erwerben oder ein eigenes Sicherheitszertifikat für die SSL-Verbindungen zu verwenden. Bei Verwenden des selbst signierten Zertifikats erhalten Clients eine Warnmeldung zum Zertifikat.

Um dieses Problem zu beheben, installieren Sie ein von einer anerkannten Zertifizierungsstelle signiertes Zertifikat.

Der Standardspeicherort für das Zertifikat ist `/etc/vmware/ssl/` auf dem ESX Server 3-Host. Das Zertifikat besteht aus zwei Dateien: dem Zertifikat selbst (`rui.crt`) und der persönlichen Schlüsseldatei (`rui.key`).

Hinzufügen von Zertifikaten und Ändern der Web-Proxyeinstellungen von ESX Server 3

Beachten Sie beim Hinzufügen von Zertifikaten zu ESX Server 3 und bei der Planung von Verschlüsselung und Benutzersicherheit Folgendes:

- Vermeiden Sie das Einrichten von Zertifikaten unter Verwendung von Kennwortsätzen. ESX Server 3 kann Kennwortsätze (verschlüsselte Schlüssel) nicht verarbeiten. Wenn Sie einen Kennwortsatz einrichten, können ESX Server 3-Prozesse nicht ordnungsgemäß starten.
- Sie können den Web-Proxy so konfigurieren, dass er an einer anderen Stelle als am Standardspeicherort nach Zertifikaten sucht. Dies ist hilfreich, wenn die Zertifikate zentral auf einem Computer gespeichert werden sollen, damit mehrere Hosts die Zertifikate verwenden können.

VORSICHT Zertifikate, die an einem anderen Speicherort als auf dem ESX Server 3-Host gespeichert werden, sind unbrauchbar, wenn der Host keine Netzwerkverbindung hat. Ist die Zertifikatsprüfung aktiviert, können Sie keine sicheren Verbindungen mit Gästen einrichten.

- Zur Unterstützung von Verschlüsselung für Benutzernamen, Kennwörter und Pakete wird SSL standardmäßig für VI Web Access- und VMware Infrastructure SDK-Verbindungen aktiviert. Wenn Sie diese Verbindungen so konfigurieren möchten, dass Übertragungen nicht verschlüsselt werden, deaktivieren Sie SSL für Ihre VI Web Access- bzw. VMware Infrastructure SDK-Verbindung, indem Sie die Verbindung von HTTPs auf HTTP umstellen (siehe „So ändern Sie Sicherheitseinstellungen für einen Web-Proxy-Dienst“ auf Seite 240). Deaktivieren Sie SSL nur dann, wenn Sie eine vollständig vertrauenswürdige Umgebung für die Clients geschaffen haben, d. h. Firewalls wurden installiert und die Übertragungen zum und vom Host sind vollständig isoliert. Die Deaktivierung von SSL kann die Leistung verbessern, da der für die Verschlüsselung notwendige Verarbeitungsaufwand nicht anfällt.
- Um den Missbrauch von ESX Server 3-Diensten wie dem internen Webserver, auf dem VI Web Access ausgeführt wird, zu verhindern, kann auf die meisten internen ESX Server 3-Dienste nur über Port 443, den für HTTPS-Übertragungen verwendeten Port, zugegriffen werden. Port 443 dient als Reverse-Proxy für ESX Server 3. Sie können eine Liste der Dienste auf dem ESX Server 3-Host auf einer HTTP-Begrüßungsseite sehen. Sie können aber nur direkt auf diese Dienste zugreifen, wenn Sie über die entsprechenden Berechtigungen verfügen. Sie können diese Einstellung ändern, sodass auf bestimmte Dienste direkt über HTTP-Verbindungen zugegriffen werden kann. VMware empfiehlt, dass Sie diese Änderung nur vornehmen, wenn Sie ESX Server 3 in einer voll vertrauenswürdigen Umgebung verwenden.

- Wenn Sie VirtualCenter und VI Web Access aktualisieren, wird das Zertifikat beibehalten. Wenn Sie VirtualCenter und VI Web Access deinstallieren, wird das Verzeichnis, in dem sich das Zertifikat befindet, nicht aus der Servicekonsole gelöscht.

So konfigurieren Sie den Web-Proxy zur Suche nach Zertifikaten an anderen Speicherorten

1 Melden Sie sich als Root-Benutzer an der Servicekonsole an.

2 Wechseln Sie zum Verzeichnis `/etc/vmware/hostd/`.

3 Öffnen Sie die Datei `proxy.xml` in einem Texteditor, und bearbeiten Sie das folgende XML-Segment:

```
<ssl>
   <!-- The server private key file -->
   <privateKey>/etc/vmware/ssl/rui.key</privateKey>
   <!-- The server side certificate file -->
   <certificate>/etc/vmware/ssl/rui.crt</certificate>
</ssl>
```

4 Ersetzen Sie `/etc/vmware/ssl/rui.key` durch den absoluten Pfad zur persönlichen Schlüsseldatei, die Sie von der vertrauenswürdigen Zertifizierungsstelle erhalten haben.

   Dieser Pfad kann sich auf dem ESX Server 3-Host oder auf einem zentralen Computer befinden, auf dem die Zertifikate und Schlüssel für Ihr Unternehmen gespeichert sind.

   HINWEIS Belassen Sie die XML-Tags `<privateKey>` und `</privateKey>` an ihrem Platz.

5 Ersetzen Sie `/etc/vmware/ssl/rui.crt` durch den absoluten Pfad zur Zertifikatsdatei, die Sie von der vertrauenswürdigen Zertifizierungsstelle erhalten haben.

VORSICHT Löschen Sie die ursprünglichen Dateien `rui.key` und `rui.crt` nicht. Der ESX Server-Host verwendet diese Dateien.

6 Speichern Sie die Änderungen, und schließen Sie die Datei.

7 Geben Sie folgenden Befehl ein, um den Prozess `vmware-hostd` neu zu starten:

```
service mgmt-vmware restart
```

So ändern Sie Sicherheitseinstellungen für einen Web-Proxy-Dienst

1 Melden Sie sich als Root-Benutzer an der Servicekonsole an.

2 Wechseln Sie zum Verzeichnis `/etc/vmware/hostd/`.

3 Bearbeiten Sie die Datei `proxy.xml` mithilfe eines Texteditors. Der Inhalt der Datei sind meist so aus:

```
<ConfigRoot>
   <EndpointList>
      <_length>6</_length>
      <_type>vim.ProxyService.EndpointSpec[]</_type>
      <e id="0">
         <_type>vim.ProxyService.NamedPipeServiceSpec</_type>
         <accessMode>httpsWithRedirect</accessMode>
         <pipeName>/var/run/vmware/proxy-webserver</pipeName>
         <serverNamespace>/</serverNamespace>
      </e>
      <e id="1">
         <_type>vim.ProxyService.NamedPipeServiceSpec</_type>
         <accessMode>httpsWithRedirect</accessMode>
         <pipeName>/var/run/vmware/proxy-sdk</pipeName>
         <serverNamespace>/sdk</serverNamespace>
      </e>
      <e id="2">
         <_type>vim.ProxyService.LocalServiceSpec</_type>
         <accessMode>httpsWithRedirect</accessMode>
         <port>8080</port>
         <serverNamespace>/ui</serverNamespace>
      </e>
      <e id="3">
         <_type>vim.ProxyService.NamedPipeServiceSpec</_type>
         <accessMode>httpsOnly</accessMode>
         <pipeName>/var/run/vmware/proxy-vpxa</pipeName>
         <serverNamespace>/vpxa</serverNamespace>
      </e>
      <e id="4">
         <_type>vim.ProxyService.NamedPipeServiceSpec</_type>
         <accessMode>httpsWithRedirect</accessMode>
         <pipeName>/var/run/vmware/proxy-sdk</pipeName>
         <serverNamespace>/mob</serverNamespace>
      </e>
      <e id="5">
         <_type>vim.ProxyService.LocalServiceSpec</_type>
         <!-- Use this mode for "secure" deployment -->
         <!-- <accessMode>httpsWithRedirect</accessMode> -->
         <!-- Use this mode for "insecure" deployment -->
         <accessMode>httpAndHttps</accessMode>
         <port>8889</port>
         <serverNamespace>/wsman</serverNamespace>
      </e>
   </EndpointList>
</ConfigRoot>
```

4 Ändern Sie die Sicherheitseinstellungen den Anforderungen entsprechend. Sie können beispielsweise die Einträge für Dienste ändern, die HTTPS verwenden, um den HTTP-Zugriff ergänzen.

   - *e id* eine ID-Nummer für das XML-Tag mit der Server-ID. ID-Nummern müssen im HTTP-Bereich eindeutig sein.
   - *_type* der Name des Dienstes, den Sie verschieben, z. B. `/sdk` oder `/mob`.
   - *accessmode* ist die Form der Kommunikation, die der Dienst zulässt. Zu den zulässigen Werten gehören u. a.:
     - **httpOnly** – Auf den Dienst kann nur über unverschlüsselte HTTP-Verbindungen zugegriffen werden.
     - **httpsOnly** – Auf den Dienst kann nur über HTTPS-Verbindungen zugegriffen werden.
     - **httpsWithRedirect** – Auf den Dienst kann nur über HTTPS-Verbindungen zugegriffen werden. Anforderungen über HTTP werden an die entsprechende HTTPS-URL weitergeleitet.
     - **httpAndHttps** – Auf den Dienst kann über HTTP- und HTTPS-Verbindungen zugegriffen werden.
   - *port* ist die Nummer des Ports, der dem Dienst zugewiesen wurde. Sie können dem Dienst eine andere Portnummer zuweisen.
   - *namespace* ist der Namensraum des Servers, der diesen Dienst bereitstellt.

5 Speichern Sie die Änderungen, und schließen Sie die Datei.

6 Geben Sie folgenden Befehl ein, um den Prozess `vmware-hostd` neu zu starten:

```
service mgmt-vmware restart
```

Beispiel: Einrichten von VI Web Access für die Kommunikation über einen unsicheren Port

VI Web Access kommuniziert mit einem ESX Server 3-Host normalerweise über einen sicheren Port (HTTPS, 443). Wenn Sie sich in einer vollständig vertrauenswürdigen Umgebung befinden, können Sie auch einen unsicheren Port verwenden (zum Beispiel HTTP, 80). Ändern Sie dazu das Attribut **accessMode** für den Webserver in der Datei `proxy.xml` (siehe „So ändern Sie Sicherheitseinstellungen für einen Web-Proxy-Dienst“ auf Seite 240). Das Ergebnis sieht folgendermaßen aus. `accessMode` wird von `httpsWithRedirect` in `httpAndHttps` geändert.

```
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpAndHttps</accessMode>
<port>8080</port>
<serverNamespace>/ui</serverNamespace>
```

Erneutes Erzeugen von Zertifikaten

Der ESX Server 3-Host erzeugt Zertifikate, wenn Sie den Host nach der Installation zum ersten Mal starten. Anschließend sucht bei jedem Neustart des Prozesses `vmware-hostd` das Skript `mgmt-vmware` nach vorhandenen Zertifikatsdateien (`rui.crt` und `rui.key`). Für den Fall, dass es keine findet, werden neue Zertifikatsdateien erzeugt.

Unter gewissen Umständen kann es sein, dass Sie den ESX Server 3-Host zwingen müssen, neue Zertifikate zu erzeugen. Typischerweise müssen Sie nur in folgenden Fällen neue Zertifikate erstellen:

- Sie ändern den Hostnamen.
- Sie löschen versehentlich die Zertifikate.

So erzeugen Sie neue Zertifikate für den ESX Server 3-Host

1 Wechseln Sie zum Verzeichnis `/etc/vmware/ssl`.

2 Erstellen Sie Sicherungskopien aller existierenden Zertifikate, indem Sie die folgenden Befehle ausführen:

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```

HINWEIS Wenn Sie Zertifikate erstellen, weil Sie zuvor Zertifikate versehentlich gelöscht haben, müssen Sie die Sicherung nicht auszuführen.

3 Geben Sie folgenden Befehl ein, um den Prozess `vmware-hostd` neu zu starten:

```
service mgmt-vmware restart
```

4 Bestätigen Sie, dass der ESX Server 3-Host neue Zertifikate erstellt hat, indem Sie den folgenden Befehl ausführen, der die Zeitstempel der neuen Zertifikatsdateien mit **orig.rui.crt** und **orig.rui.key** vergleicht:

```
ls -la
```

Delegierte VM-Benutzer für NFS-Speicher

Für die meisten Vorgänge auf virtuellen Maschinen benötigt ein ESX Server 3-Host Zugriff auf die Dateien der virtuellen Maschine. So muss der ESX Server 3-Host zum Beispiel zum Hoch- oder Herunterfahren virtueller Maschinen Dateien auf dem Datenträger, auf dem die Dateien der virtuellen Festplatte gespeichert sind, erstellen, bearbeiten und löschen können.

Wenn Sie virtuelle Maschinen in einem NFS-basierten Datenspeicher erstellen, konfigurieren oder verwalten möchten, können Sie den so genannten delegierten Benutzer verwenden. Die Identität des delegierten Benutzers wird von ESX Server 3i für den gesamten Datenverkehr zum und vom zugrunde liegenden Dateisystem verwendet. Der delegierte Benutzer ist experimentell und wird nicht offiziell unterstützt.

Der delegierte Benutzer für den ESX Server 3-Host ist standardmäßig `root`. Nicht alle NFS-Datenspeicher akzeptieren jedoch `Root` als delegierten Benutzer. NFS-Administratoren können Volumes mit aktivierter Option **root squash (root squashing)** exportieren. Die Funktion `root squash` ordnet den Root-Benutzer einem Benutzer ohne wesentliche Berechtigungen auf dem NFS-Server zu und beschränkt so die Berechtigungen des Root-Benutzers. Diese Funktion dient meistens dazu, unerlaubte Zugriffe auf Dateien auf dem NFS-Volume zu verhindern. Wenn das NFS-Volume mit aktivierter Option `root squash` exportiert wurde, kann es sein, dass der NFS-Server den Zugriff auf den ESX Server 3-Host verweigert. Um sicherzustellen, dass Sie virtuelle Maschinen über Ihren Host anlegen und verwalten können, muss der NFS-Administrator die Funktion `Root–Squash` deaktivieren oder den physischen Netzwerkadapter des ESX Server 3-Hosts der Liste der vertrauten Server hinzufügen.

Wenn der NFS-Administrator keine dieser beiden Aktionen durchführen möchte, können Sie den delegierten Benutzer durch die experimentellen ESX Server 3-Funktionen auf eine andere Identität setzen. Diese Identität muss mit der Identität des Besitzers des Verzeichnisses auf dem NFS-Server übereinstimmen. Ansonsten kann der ESX Server 3-Host keine Vorgänge auf Dateiebene durchführen. Um einem delegierten Benutzer eine andere Identität zuzuweisen, benötigen Sie die folgenden Informationen:

- Benutzername des Verzeichnisinhabers
- Benutzer-ID (UID) des Verzeichnisbesitzers
- Gruppen-ID (GID) des Verzeichnisbesitzers

Verwenden Sie diese Informationen, um die Einstellungen des delegierten Benutzers für den ESX Server 3-Host so zu ändern, dass sie mit den Daten des Verzeichnisbesitzers übereinstimmen. Dadurch kann der NFS-Datenspeicher den ESX Server 3-Host ordnungsgemäß erkennen. Der delegierte Benutzer wird global konfiguriert, und dieselbe Identität wird zum Zugriff auf jedes Volume verwendet.

Die Einrichtung des delegierten Benutzer auf einem ESX Server 3-Host umfasst folgende Schritte:

- Aus der Registerkarte **Benutzer und Gruppen (Users & Groups)** für einen VI-Client, der direkt auf einem ESX Server 3-Host ausgeführt wird, haben Sie zwei Möglichkeiten:
  - Bearbeiten Sie den Benutzernamen `vimuser`, um die ordnungsgemäße UID und GID einzugeben. Bei `vimuser` handelt es sich um einen Benutzer des ESX Server 3-Hosts, der bereitgestellt wird, um Ihnen die Einrichtung delegierter Benutzer zu vereinfachen. Standardmäßig hat `vimuser` die UID 12 und die GID 20.
  - Fügen Sie einen komplett neuen Benutzer dem ESX Server 3-Host hinzu. Dazu geben Sie den Namen des delegierten Benutzers, die UID und die GID an.

  Sie müssen einen dieser Schritte ausführen und dies unabhängig davon, ob Sie den Host über eine direkte Verbindung oder VirtualCenter Server verwalten. Außerdem müssen Sie sicherstellen, dass der delegierte Benutzer (`vimuser` oder der delegierte Benutzer, den Sie einrichten) auf allen ESX Server 3-Hosts identisch ist, die den NFS-Datenspeicher verwenden. Informationen zum Hinzufügen von Benutzern erhalten Sie unter „Verwalten der Tabelle „Benutzer““ auf Seite 231.
- Konfigurieren Sie einen delegierten Benutzer für virtuelle Maschinen als Teil des Sicherheitsprofils für den Host (siehe unten). Konfigurieren Sie das Sicherheitsprofil über VirtualCenter oder einen VI-Client, der direkt auf dem ESX Server 3-Host ausgeführt wird.

WARNUNG Das Ändern eines delegierten Benutzers für einen ESX Server 3-Host ist experimentell. Derzeit unterstützt VMware diese Implementierung nicht. Die Verwendung dieser Funktion kann zu einem unerwarteten Verhalten des Hosts führen.

So ändern Sie den delegierten VM-Benutzer

1. Melden Sie sich über den ESX Server 3-Host am VI-Client an.
2. Wählen Sie den Server in der Bestandsliste aus.

   Die Hardwarekonfiguration für diesen Server wird auf der Registerkarte **Übersicht (Summary)** angezeigt.
3. Klicken Sie auf **In den Wartungsmodus wechseln (Enter Maintenance Mode)**.
4. Klicken Sie auf die Registerkarte **Konfiguration (Configuration)** und dann auf **Sicherheitsprofil (Security Profile)**.

5 Klicken Sie auf **Delegierter für virtuelle Maschine (Virtual Machine Delegate) > Bearbeiten (Edit)**. Das Dialogfeld **Delegierter für virtuelle Maschine (Virtual Machine Delegate)** wird angezeigt.

6 Geben Sie den Benutzernamen des delegierten Benutzers ein.

7 Klicken Sie auf **OK**.

8 Starten Sie den ESX Server 3-Host neu.

Nach dem Neustart des Hosts wird die Einstellung des delegierten Benutzers sowohl in VirtualCenter als auch im direkt auf dem ESX Server 3-Host ausgeführten VI-Client angezeigt.

Sicherheit der Servicekonsole 12

Dieses Kapitel enthält grundlegende Sicherheitsempfehlungen für die Servicekonsole und erläutert einige der in die Servicekonsole integrierten Sicherheitsfunktionen. Die Servicekonsole ist eine Verwaltungsschnittstelle für ESX Server 3. Daher ist ihre Sicherheit sehr wichtig. Um die Servicekonsole gegen unbefugten Zugriff und Missbrauch zu schützen, beschränkt VMware bestimmte Parameter, Einstellungen und Aktivitäten der Servicekonsole.

Diese Beschränkungen wurden dazu entworfen, die Sicherheit für ESX Server 3 zu erhöhen. Sie können diese Beschränkungen lockern, um Ihre spezifischen Konfigurationsbedürfnisse zu erfüllen. In diesem Fall müssen Sie aber tatsächlich in einer vertrauenswürdigen Umgebung arbeiten und genügend andere Sicherheitsmaßnahmen ergriffen haben, um das Netzwerk als Ganzes und die an den ESX Server 3-Host angeschlossenen Geräte zu schützen.

In diesem Kapitel werden folgende Themen behandelt:

- „Allgemeine Sicherheitsempfehlungen“ auf Seite 248
- „Konfiguration der Servicekonsolen-Firewall“ auf Seite 249
- „Kennwortbeschränkungen“ auf Seite 254
- „Schlüsselqualität“ auf Seite 262
- „setuid- und setgid-Anwendungen“ auf Seite 263
- „SSH-Sicherheit“ auf Seite 265
- „Sicherheitspatches und Software zum Suchen nach Sicherheitslücken“ auf Seite 267

Allgemeine Sicherheitsempfehlungen

Beachten Sie bei der Überprüfung der Servicekonsolensicherheit und der Verwaltung der Servicekonsole folgende Sicherheitsempfehlungen:

- **Beschränken Sie den Benutzerzugriff.**

  Beschränken Sie zur Verbesserung der Sicherheit den Benutzerzugriff auf die Servicekonsole, und legen Sie weitere Sicherheitsbeschränkungen fest, wie z. B. Kennwortrestriktionen (Vorgabe der Kennwortlänge, Zeitbeschränkung der Kennwörter, Verwendung eines `grub`-Kennworts beim Hochfahren des Hosts).

  Die Servicekonsole hat privilegierten Zugriff auf bestimmte Teile von ESX Server 3. Daher sollten nur vertrauenswürdige Benutzer Zugriff darauf erhalten. In der Standardeinstellung ist der Root-Zugriff beschränkt, wodurch eine SSH-Anmeldung (Secure Shell) als Root nicht möglich ist. Wir empfehlen, diese Standardeinstellung beizubehalten. Administratoren von ESX Server 3-Systemen sollten sich als normale Benutzer anmelden müssen und dann den Befehl `sudo` ausführen, um bestimmte Aufgaben, die Root-Berechtigungen erfordern, auszuführen.

  Versuchen Sie auch, so wenige Prozesse wie möglich auf der Servicekonsole auszuführen. Im Idealfall sollten nur die wichtigen Prozesse, Dienste und Agenten ausgeführt werden, z. B. Antivirenprogramme, Sicherungen virtueller Maschinen usw.

- **Verwalten Sie ESX Server 3-Hosts über den VI-Client.**

  Verwenden Sie den VI-Client, VI Web Access oder, wenn dies möglich ist, ein Netzwerkverwaltungsprogramm eines anderen Anbieters zur Verwaltung der ESX Server 3-Hosts, anstatt als Root-Benutzer über die Befehlszeilenoberfläche zu agieren. Mit dem VI-Client können Sie die Anzahl an Konten, die Zugriff auf die Servicekonsole haben, einschränken, Zuständigkeiten sicher weitergeben und Rollen einrichten, damit Administratoren und Benutzer keine Funktionen nutzen können, die sie nicht benötigen.

- **Verwendung Sie nur VMware-Quellen für Aktualisierungen von ESX Server 3-Komponenten, die auf der Servicekonsole ausgeführt werden.**

  Auf der Servicekonsole werden zur Unterstützung erforderlicher Verwaltungsschnittstellen oder -aufgaben viele Pakete anderer Anbieter, zum Beispiel der Web-Dienst Tomcat, ausgeführt. Bei VMware dürfen diese Pakete nur über eine VMware-Quelle aktualisiert werden. Wenn Sie einen Download oder Patch aus einer anderen Quelle verwenden, können die Sicherheit und die Funktionen der Servicekonsole gefährdet werden. Überprüfen Sie die Internetseiten von Drittanbietern und die VMware-Wissensdatenbank regelmäßig auf Sicherheitswarnungen.

Anmelden an der Servicekonsole

Obwohl die meisten Konfigurationsvorgänge für ESX Server 3 über den VI-Client ausgeführt werden, müssen bestimmte Sicherheitsfunktionen über die Befehlszeilenoberfläche der Servicekonsole konfiguriert werden. Zur Verwendung der Befehlszeilenoberfläche müssen Sie sich am Host anmelden. Wenn Sie direkten Zugriff auf den ESX Server 3-Host haben, können Sie sich an der physischen Konsole auf diesem Computer anmelden. Drücken Sie dazu auf dem Anmeldebildschirm ALT-F2. Verwenden Sie bei Remoteverbindungen mit der Konsole SSH oder eine andere Remotesteuerungsverbindung, um eine Sitzung auf dem Host zu starten.

In beiden Fällen, sowohl bei der lokalen Anmeldung als auch bei der Anmeldung über eine Fernverbindung wie SSH, müssen Sie sich mit einem Benutzernamen und einem Kennwort anmelden, den/das der ESX Server 3-Host erkennt. Weitere Informationen zu Benutzernamen und Kennwörtern für ESX Server 3-Hosts finden Sie unter „Verwalten von Benutzern und Gruppen auf ESX Server 3-Hosts“ auf Seite 230.

Wenn Sie sich auf dem Host anmelden, um Vorgänge auszuführen, für die Root-Berechtigungen notwendig sind, sollten Sie sich zuerst als normaler Benutzer an der Servicekonsole anmelden und dann über den Befehl `su` oder den zu bevorzugenden Befehl `sudo` als Root anmelden. Der Befehl `sudo` erhöht die Sicherheit, da er nur für bestimmte, ausgewählte Vorgänge Root-Berechtigungen gewährt, während `su` Root-Berechtigungen für alle Vorgänge gewährt. Bei Verwenden von `sudo` sind außerdem alle Vorgänge besser nachvollziehbar, da alle `sudo`-Vorgänge protokolliert werden, wohingegen bei Verwenden von `su` ESX Server 3 nur protokolliert, dass der Benutzer durch `su` auf Root umgeschaltet hat.

Zusätzlich zu den ESX-spezifischen Befehlen können Sie über die Befehlszeilenoberfläche der Servicekonsole auch viele Linux- und UNIX-Befehle ausführen. Detaillierte Hinweise zu Servicekonsolenbefehlen erhalten Sie über den Befehl `man <Befehlsname>`, mit dem Sie die Hilfeseiten aufrufen.

Konfiguration der Servicekonsolen-Firewall

ESX Server 3 bietet eine Firewall zwischen der Servicekonsole und dem Netzwerk. Damit die Integrität der Servicekonsole sichergestellt ist, hat VMware die Anzahl an standardmäßig freigegebenen Firewall-Ports reduziert. Bei der Installation wird die Firewall der Servicekonsole so konfiguriert, dass der gesamte ein- und ausgehende Datenverkehr auf allen Ports außer auf 902, 443, 80 und 22 blockiert wird. Die genannten Ports werden für die grundlegende Kommunikation mit ESX Server 3 verwendet. Durch diese Einstellung ist die Sicherheitsstufe für den ESX Server 3-Host sehr hoch.

HINWEIS Die Firewall lässt auch Internet Control Message Protocol (ICMP)-Pings und Kommunikation mit DHCP- und DNS- Clients (nur UDP) zu.

In vertrauenswürdigen Umgebungen kann eine niedrigere Sicherheitsstufe möglich sein. In diesem Fall können Sie die Firewall entweder auf mittlere oder niedrige Sicherheit setzen:

- **Mittlere Sicherheit** – Der gesamte eingehende Datenverkehr wird blockiert, ausgenommen ist Datenverkehr auf den Standard-Ports (902, 433, 80 und 22) sowie auf allen Ports, die Sie freigeben. Ausgehender Datenverkehr wird nicht blockiert.
- **Niedrige Sicherheit** – Weder eingehender noch ausgehender Datenverkehr wird blockiert. Diese Einstellung entspricht der Deaktivierung der Firewall.

Da die standardmäßig freigegebenen Ports stark beschränkt sind, müssen Sie ggf. nach der Installation zusätzliche Ports freigeben. Eine Liste häufig verwendeter Ports, die Sie ggf. freigeben müssen, finden Sie unter „TCP- und UDP-Ports für den Verwaltungszugriff“ auf Seite 193.

Durch Hinzufügen unterstützter Dienste und Verwaltungs-Agenten, die zum effektiven Betrieb von ESX Server 3 notwendig sind, werden weitere Ports in der Firewall der Servicekonsole freigegeben. Dienste und Verwaltungs-Agenten werden über VirtualCenter hinzugefügt (siehe „Öffnen von Firewallports für unterstützte Dienste und Verwaltungs-Agenten“ auf Seite 198).

Neben den Ports, die für diese Dienste und Agenten freigegeben werden, müssen Sie eventuell andere Ports freigeben, wenn Sie bestimmte Geräte, Dienste oder Agenten, z. B. Speichergeräte, Sicherungs- oder Verwaltungs-Agenten, konfigurieren. Wenn Sie zum Beispiel Veritas NetBackup™ 4.5 als Sicherungs-Agenten verwenden, müssen Sie die Ports 13720, 13724, 13782 und 13783 freigeben, die NetBackup für Client-Medien-Übertragungen, Datenbanksicherungen, Benutzersicherungen und -wiederherstellungen usw. verwendet. Informationen zu den für bestimmte Anwendungen freizugebenden Ports finden Sie in den Herstellerspezifikationen für das Gerät, den Dienst oder den Agenten.

Ändern der Sicherheitsstufe der Servicekonsole

Die Änderung der Sicherheitsstufe für die Servicekonsole umfasst zwei Schritte: Bestimmen der Sicherheitsstufe der Servicekonsolen-Firewall und Zurücksetzen der Einstellungen der Servicekonsolen-Firewall. Um überflüssige Schritte zu vermeiden, überprüfen Sie immer die Firewalleinstellungen, bevor Sie sie ändern.

Jedes Mal, wenn Sie die Sicherheitseinstellung senken oder zusätzliche Ports öffnen, erhöhen Sie das Risiko eines Eindringens in Ihr Netzwerk. Wägen Sie genau ab, wie wichtig Ihnen Zugriffsrechte im Kontrast zur Sicherheit des Netzwerks sind.

So bestimmen Sie die Sicherheitsstufe der Servicekonsolen-Firewall

1 Melden Sie sich an der Servicekonsole an, und rufen Sie Root-Berechtigungen ab.

2 Führen Sie die beiden folgenden Befehle aus, um zu bestimmen, ob ein- und ausgehender Datenverkehr erlaubt oder blockiert wird:

```
esxcfg-firewall -q incoming
esxcfg-firewall -q outgoing
```

3 Die Ergebnisse bedeuten Folgendes:

Tabelle 12-1. Sicherheitsstufen der Servicekonsole

Befehlszeilenausgabe	Sicherheitsstufe
`Incoming ports blocked by default.` `Outgoing ports blocked by default.`	Hoch
`Incoming ports blocked by default.` `Outgoing ports not blocked by default.`	Mittel
`Incoming ports not blocked by default.` `Outgoing ports not blocked by default.`	Niedrig

So legen Sie die Sicherheitsstufe der Servicekonsolen-Firewall fest

1 Melden Sie sich an der Servicekonsole an, und rufen Sie Root-Berechtigungen ab.

2 Führen Sie je nach Bedarf einen der folgenden Befehle aus.

- So legen Sie die mittlere Sicherheitsstufe für die Servicekonsolen-Firewall fest:

  ```
  esxcfg-firewall --allowOutgoing --blockIncoming
  ```

- So legen Sie die niedrige Sicherheitsstufe für die virtuelle Firewall fest:

  ```
  esxcfg-firewall --allowIncoming --allowOutgoing
  ```

VORSICHT Der vorherige Befehl deaktiviert den Schutz durch die Firewall vollständig.

- So legen Sie die hohe Sicherheitsstufe für die Servicekonsolen-Firewall fest:

  ```
  esxcfg-firewall --blockIncoming --blockOutgoing
  ```

3 Geben Sie folgenden Befehl ein, um den Prozess `vmware-hostd` neu zu starten:

```
service mgmt-vmware restart
```

Die Änderung der Sicherheitsstufe der Servicekonsolen-Firewall beeinflusst bestehende Verbindungen nicht. Wenn die Firewall zum Beispiel auf niedriger Sicherheitsstufe ausgeführt wird und an einem Port, den Sie nicht ausdrücklich freigegeben haben, eine Sicherung ausgeführt wird, beendet eine Erhöhung der Sicherheitsstufe auf „Hoch“ die Sicherung nicht. Weil die Firewall so konfiguriert ist, dass die Pakete für zuvor hergestellte Verbindungen durchgelassen werden, wird die Sicherung abgeschlossen und die neue Verbindung freigegeben. Anschließend werden für diesen Port keine weiteren Verbindungen akzeptiert.

Freigeben und Blockieren von Ports in der Servicekonsolen-Firewall

Wenn Sie Geräte, Dienste oder Agenten anderer Anbieter installieren, können Sie Ports in der Servicekonsolen-Firewall freigeben. Bevor Sie Ports für das Gerät oder den Dienst freigeben, konsultieren Sie die Herstellerspezifikationen, um zu bestimmen, welche Ports freigegeben werden müssen.

Wenn Sie einen Port blockieren, werden aktive Sitzungen des Dienstes, der den Port verwendet, nicht automatisch getrennt, sobald Sie den Port blockieren. Wenn Sie zum Beispiel eine Sicherung durchführen und Sie den Port für den Sicherungs-Agenten schließen, wird die Sicherung bis zum Abschluss fortgesetzt und der Agent die Verbindung freigibt.

Verwenden Sie die folgenden Verfahren nur, wenn Sie Ports für Dienste oder Agenten freigeben oder blockieren, die nicht über den VI-Client konfiguriert werden können. Informationen zur Konfiguration zusätzlicher Ports in VirtualCenter finden Sie unter „Öffnen von Firewallports für unterstützte Dienste und Verwaltungs-Agenten“ auf Seite 198.

VORSICHT VMware Support unterstützt das Öffnen und Blockieren der Firewallports nur über den VI-Client oder den Befehl `esxcfg-firewall` (siehe unten). Eine Verwendung anderer Methoden oder Skripts zum Öffnen oder Blockieren der Firewallports kann zu einem unerwarteten Verhalten führen.

So öffnen Sie einen bestimmten Port in der Firewall der Servicekonsole

1 Melden Sie sich an der Servicekonsole an, und rufen Sie Root-Berechtigungen ab.

2 Führen Sie den folgenden Befehl aus:

```
esxcfg-firewall --openPort <Portnummer>,tcp|udp,in|out,<Portname>
```

wobei:

- `Portnummer` die vom Hersteller angegebene Portnummer ist.

- `tcp|udp` das Protokoll ist. Geben Sie `tcp` für TCP-Datenverkehr oder `udp` für UDP-Datenverkehr an.
- `in|out` ist die Richtung des Datenverkehrs. Geben Sie `in` an, um einen Port für eingehenden Datenverkehr freizugeben, oder `out`, um den Port für ausgehenden Datenverkehr zu öffnen.
- `Portname` ist ein beschreibender Name. Der Name muss nicht eindeutig sein, sollte jedoch aussagekräftig sein, damit der Dienst oder Agent identifiziert werden kann, der den Port verwendet.

  Beispiel:

  ```
  esxcfg-firewall --openPort 6380,tcp,in,Navisphere
  ```

3 Geben Sie folgenden Befehl ein, um den Prozess `vmware-hostd` neu zu starten:

```
service mgmt-vmware restart
```

So blockieren Sie einen bestimmten Port in der Servicekonsolen-Firewall

1 Melden Sie sich an der Servicekonsole an, und rufen Sie Root-Berechtigungen ab.

2 Führen Sie den folgenden Befehl aus:

```
esxcfg-firewall --closePort <Portnummer>,tcp|udp,in|out,<Portname>
```

Für den Befehl `-closePort` ist das Argument `Portname` optional.

Beispiel:

```
esxcfg-firewall --closePort 6380,tcp,in
```

3 Geben Sie folgenden Befehl ein, um den Prozess `vmware-hostd` neu zu starten:

```
service mgmt-vmware restart
```

Sie können die Option `-closePort` verwenden, um nur die Ports zu blockieren, die Sie mit der Option `-openPort` freigegeben hatten. Wenn Sie ein anderes Verfahren verwendet haben, um den Port freizugeben, müssen Sie auch das entsprechende Gegenstück zu dem Verfahren verwenden, um ihn zu blockieren. So können Sie zum Beispiel den SSH-Port (22) nur blockieren, indem Sie die ein- und ausgehende SSH-Server-Verbindung im VI-Client deaktivieren. Weitere Informationen zur Freigabe und Blockierung von Ports über den VI-Client finden Sie unter „Öffnen von Firewallports für unterstützte Dienste und Verwaltungs-Agenten“ auf Seite 198.

Kennwortbeschränkungen

Wie mühelos sich ein Angreifer an einem ESX Server 3-Host anmelden kann, hängt davon ab, wie schnell er eine gültige Benutzername-/Kennwort-Kombination finden kann. Ein böswilliger Benutzer kann sich ein Kennwort auf verschiedene Arten verschaffen. Zum Beispiel kann er unsicheren Netzwerkdatenverkehr wie z. B. Telnet- oder FTP-Übertragungen auf erfolgreiche Anmeldeversuche überwachen.

Ein anderes häufig verwendetes Verfahren zum Knacken eines Kennwortes ist die Verwendung eines Kennwortgenerators. Kennwortgeneratoren können für verschiedene Kennwortangriffe verwendet werden, z. B. Brute-Force-Angriffe, bei denen der Generator alle möglichen Zeichenkombinationen bis zu einer bestimmten Kennwortlänge ausprobiert, und Wörterbuchangriffe, bei denen der Generator existierende Wörter und einfache Abwandlungen existierender Wörter ausprobiert.

Der Einsatz von Beschränkungen bezüglich der Länge, der verwendeten Zeichen und der Verwendungsdauer eines Kennwortes kann Angriffe durch Kennwortgeneratoren schwieriger gestalten. Je länger und komplexer ein Kennwort ist, desto schwieriger ist es für einen Angreifer, das Kennwort herauszufinden. Je öfter Benutzer ihre Kennwörter ändern müssen, desto schwieriger ist es, ein Kennwort zu finden, das mehrmals funktioniert.

HINWEIS Denken Sie immer an mögliche menschliche Fehler, wenn Sie die Kennworteinschränkungen festlegen. Wenn Sie Kennwörter verlangen, die man sich kaum merken kann oder häufige Änderungen vorschreiben, kann es sein, dass die Benutzer ihre Kennwörter aufschreiben müssen und dadurch das gewünschte Ziel aushebeln.

Zum Schutz der Kennwortdatenbank gegen Missbrauch wurde Kennwort-Shadowing für ESX Server 3 aktiviert, sodass die Kennwort-Hashes zugriffsgeschützt sind. Außerdem verwendet ESX Server 3 MD5-Kennwort-Hashes, die eine höhere Kennwortsicherheit bieten und es ermöglichen, Kennwörter mit einer Mindestlänge von mehr als 8 Zeichen anzufordern.

ESX Server 3 bietet eine Kennwortkontrolle auf zwei Ebenen, um Kennwortrichtlinien für Benutzer durchzusetzen und das Risiko des Knackens von Kennwörtern zu begrenzen:

- **Kennwortverwendungsdauer** – Diese Einstellungen bestimmen, wie lange ein Benutzerkennwort aktiv sein kann, bevor der Benutzer es ändern muss. Dadurch wird sichergestellt, dass das Kennwort oft genug geändert wird, sodass ein Angreifer, der ein Kennwort durch Ausspionieren oder soziale Kontakte erhalten hat, nicht auf unbestimmte Zeit auf ESX Server 3 zugreifen kann.
- **Kennwortkomplexität** – Diese Einstellung stellt sicher, dass Benutzer Kennwörter auswählen, die für Kennwortgeneratoren schwer zu bestimmen sind.

Kennwortverwendungsdauer

Damit Kennwörter für die Benutzeranmeldung nicht für lange Zeiträume aktiv bleiben, werden standardmäßig folgende Beschränkungen für die Verwendungsdauer von ESX Server 3 auferlegt:

- **Höchstanzahl von Tagen** – Die Anzahl an Tagen, die ein Benutzer ein Kennwort verwenden kann, bevor es geändert werden muss. Die Standardeinstellung für ESX Server 3 ist 90 Tage. Das Konto `root` und andere Dienstkonten sind von dieser Einstellung standardmäßig ausgenommen.
- **Mindestanzahl von Tagen** – Die Mindestanzahl von Tagen, die zwischen zwei Kennwortänderungen verstreichen muss. Die Standardeinstellung lautet 0, d. h. die Benutzer können ihre Kennwörter jederzeit ändern.
- **Warnhinweiszeit** – ESX Server 3 gibt eine bestimmte Anzahl an Tagen vor Ablauf des Kennwortes einen Hinweis zur Kennwortänderung. Die Standardeinstellung ist 7 Tage. Es werden bei direkten Anmeldungen an der Servicekonsole oder bei einer Verwendung von SSH stets Warnhinweise angezeigt.

Sie können diese Einstellungen mit den Befehlsoptionen von `esxcfg-auth` verschärfen oder lockern. Verwenden Sie den Befehl `chage`, wenn die Verwendungsdauer für einen einzelnen Benutzer geändert werden soll.

So ändern Sie die Standardverwendungsdauer von Kennwörtern für ESX Server 3

1 Melden Sie sich an der Servicekonsole an, und rufen Sie Root-Berechtigungen ab.

2 Führen Sie nach Bedarf einen oder mehrere der folgenden Befehle aus.

- So ändern Sie die Höchstanzahl von Tagen, die ein Benutzer sein Kennwort behalten kann:

  ```
  esxcfg-auth --passmaxdays=<Anzahl der Tage>
  ```

  wobei `<Anzahl der Tage>` die Höchstanzahl von Tagen vor Ablauf des Kennworts ist.

- So ändern Sie die Mindestanzahl von Tagen zwischen zwei Kennwortänderungen:

  ```
  esxcfg-auth --passmindays=<Anzahl der Tage>
  ```

  wobei `<Anzahl der Tage>` die Mindestanzahl von Tagen zwischen zwei Kennwortänderungen ist.

- So ändern Sie die Hinweiszeit vor einer Kennwortänderung:

  ```
  esxcfg-auth --passwarnage=<Anzahl der Tage>
  ```

wobei <Anzahl der Tage> die Anzahl der Tage ist, die ein Benutzer vor dem Auslaufen eines Kennwortes Warnhinweise erhält.

So heben Sie die Standardverwendungsdauer von Kennwörtern für einzelne Benutzer oder Gruppen auf

1 Melden Sie sich an der Servicekonsole an, und rufen Sie Root-Berechtigungen ab.

2 Führen Sie nach Bedarf einen oder mehrere der folgenden Befehle aus.

- So geben Sie einen neuen Wert für die Höchstanzahl von Tagen an:

  ```
  chage –M <Anzahl der Tage> <Benutzername>
  ```

- So geben Sie einen neuen Wert für die Mindestanzahl von Tagen an:

  ```
  chage –m <Anzahl der Tage> <Benutzername>
  ```

- So geben Sie einen neuen Wert für die Warnhinweiszeit an:

  ```
  chage –W <Anzahl der Tage> <Benutzername>
  ```

  Weitere Informationen zu diesen und anderen Optionen des Befehls `chage` erhalten Sie über den Befehl `man chage`.

Kennwortkomplexität

Standardmäßig verwendet ESX Server das Plug-In `pam_cracklib.so` zur Festlegung der Regeln, die Benutzer bei der Erstellung von Kennwörtern beachten müssen, und zur Überprüfung der Kennwortqualität im Erstellungsprozess.

Das Plug-In `pam_cracklib.so` ermöglicht es Ihnen, Standards festzulegen, die alle Kennwörter erfüllen müssen. In der Standardeinstellung wendet ESX Server 3 keine Beschränkungen auf das Root-Kennwort an. Wenn jedoch andere Benutzer als der Root-Benutzer versuchen, ihr Kennwort zu ändern, müssen die Kennwörter, die sie auswählen, die Standards von `pam_cracklib.so` erfüllen. Außerdem können Benutzer (Root-Benutzer ausgenommen) nur eine bestimmte Anzahl an Kennwortänderungsversuchen vornehmen, bevor `pam_cracklib.so` eine Warnmeldung ausgibt und schließlich das Dialogfeld zur Änderung des Kennwortes schließt. Es gelten für ESX Server 3 folgende Kennwortstandards und Versuchsbeschränkungen für `pam_cracklib.so`:

- **Mindestlänge** – Der Mindestlängenparameter von `pam_cracklib.so` für ESX Server 3-Systeme ist auf 9 festgelegt. Dies bedeutet, dass der Benutzer mindestens acht Zeichen eingeben muss, wenn nur eine Zeichenklasse verwendet wird (Kleinbuchstaben, Großbuchstaben, Zahlen oder Sonderzeichen).

  Der Algorithmus für die Kennwortlänge lässt kürzere Kennwörter zu, wenn der Benutzer eine Mischung verschiedener Zeichenklassen zulässt. Zur Berechnung der tatsächlichen Zeichenlänge, die ein Benutzer eingeben muss, um ein gültiges

Kennwort für eine bestimmte Mindestlängeneinstellung zu erhalten, gilt folgender Kennwortlängenalgorithmus:

M – CC = E

wobei:

- M der Mindestlängenparameter ist.
- CC die Anzahl an Zeichenklassen ist, die der Benutzer für das Kennwort verwendet.
- E die Anzahl an Zeichen ist, die der Benutzer eingeben muss.

Tabelle 12-2 zeigt, wie der Algorithmus funktioniert, wenn ein Benutzer mindestens einen Kleinbuchstaben als Teil des Kennwortes eingibt. Das Plug-In `pam_cracklib.so` lässt keine Kennwörter mit weniger als sechs Zeichen zu. Daher ist zwar die mathematisch korrekte Anforderung für ein Kennwort mit vier verschiedenen Zeichenklassen fünf Zeichen, die tatsächliche Anforderung ist jedoch sechs Zeichen.

Tabelle 12-2. Ergebnisse des Kennwortkomplexitätsalgorithmus

	Zeichenklassen im Kennwortversuch			
Anzahl an Zeichen für ein gültiges Kennwort	**Kleinbuchstaben**	**Großbuchstaben**	**Zahlen**	**Andere Zeichen**
8	Ja			
7	Ja	Ja		
	Ja		Ja	
	Ja			Ja
6	Ja	Ja	Ja	
	Ja	Ja		Ja
	Ja		Ja	Ja
5	Ja	Ja	Ja	Ja

- **Wiederholungen** – Der Wiederholungsparameter von `pam_cracklib.so` für ESX Server 3-Systeme ist auf 3 festgelegt. Wenn der Benutzer bei drei Versuchen kein gültiges Kennwort eingibt, schließt `pam_cracklib.so` das Dialogfeld zur Kennwortänderung. Der Benutzer muss eine neue Sitzung zur Änderung des Kennwortes öffnen, um es erneut zu versuchen.

`pam_cracklib.so` überprüft alle Kennwortänderungsversuche, damit das Kennwort folgende Qualitätskriterien erfüllt:

- Das neue Kennwort darf kein Palindrom sein, d. h. ein Kennwort, das von hinten nach vorn und von vorn nach hinten gelesen werden kann, z. B. Radar oder Anna.
- Das neue Kennwort darf keine Umkehrung des alten Kennwortes sein.
- Das neue Kennwort darf keine Buchstabenverdrehung sein, d. h. eine Version des alten Kennwortes, in dem einer oder mehrere Buchstaben nach vorn oder hinten in der Zeichenkette verschoben wurden.
- Das neue Kennwort muss sich vom alten Kennwort durch mehr als nur durch Groß- und Kleinschreibung unterscheiden.
- Das neue Kennwort muss sich vom alten Kennwort durch mehr als nur durch einige Zeichen unterscheiden.
- Das neue Kennwort darf nicht in der Vergangenheit verwendet worden sein. `pam_cracklib.so` wendet dieses Kriterium nur an, wenn Sie eine Regel zur Wiederverwendung von Kennwörtern definiert haben.

  In der Standardeinstellung verwendet ESX Server 3 keine Regeln zur Wiederverwendung von Kennwörtern, sodass `pam_cracklib.so` normalerweise eine Kennwortänderung nicht aus diesem Grund ablehnt. Sie können jedoch eine solche Regel konfigurieren, damit Benutzer nicht nur einige wenige Kennwörter abwechselnd verwenden.

  Wenn Sie eine Regel zur Wiederverwendung von Kennwörtern konfigurieren, werden die alten Kennwörter in einer Datei gespeichert, die `pam_cracklib.so` bei jedem Kennwortänderungsversuch abfragt. Die Wiederverwendungsregeln bestimmen die Anzahl alter Kennwörter, die ESX Server 3 speichert. Wenn ein Benutzer genügend Kennwörter erstellt hat und somit der in der Regel festgelegte Wert erreicht wird, werden die alten Kennwörter anhand ihres Alters aus der Datei gelöscht. Informationen zur Konfiguration der Regel zur Wiederverwendung von Kennwörtern finden Sie unter „So konfigurieren Sie eine Regel zur Wiederverwendung von Kennwörtern“ auf Seite 259.
- Das neue Kennwort muss lang und komplex genug sein. Die Anforderungen werden durch Änderung des Komplexitätsparameter von `pam_cracklib.so` mit dem Befehl `esxcfg-auth` konfiguriert. Dieser Befehl ermöglicht Ihnen die Festlegung der Wiederholungsversuche, der Mindestkennwortlänge und verschiedener Zeichenboni. Zeichenboni ermöglichen es den Benutzern, kürzere Kennwörter einzugeben, wenn sich mehrere Zeichenarten in einem Kennwort befinden. Weitere Informationen zur Konfiguration von Kennwortlänge und Komplexität finden Sie unter „So ändern Sie Standardkomplexität von Kennwörtern für das Plug-In „pam_cracklib.so““ auf Seite 259.

Weitere Informationen zum Plug-In `pam_cracklib.so` finden Sie in der Linux-Dokumentation.

HINWEIS Das in Linux verwendete Plug-In `pam_cracklib.so` bietet mehr Parameter als die Parameter, die von ESX Server 3 unterstützt werden. Sie können diese zusätzlichen Parameter nicht in `esxcfg-auth` angeben.

So konfigurieren Sie eine Regel zur Wiederverwendung von Kennwörtern

1 Melden Sie sich an der Servicekonsole an, und rufen Sie Root-Berechtigungen ab.

2 Wechseln Sie an der Eingabeaufforderung über den Befehl `cd /etc/pam.d/` das Verzeichnis.

3 Bearbeiten Sie die Datei `system-auth` mithilfe eines Texteditors.

4 Gehen Sie zu der Zeile, die mit folgendem Argument beginnt:

```
password    sufficient    /lib/security/$ISA/pam_unix.so
```

5 Fügen Sie am Ende der Zeile folgende Parameter ein:

```
remember=X
```

Hierbei ist `X` die Anzahl der alten Kennwörter, die für jeden Benutzer gespeichert werden soll. Trennen Sie den vorhergehenden Parameter und `remember=X` durch ein Leerzeichen.

6 Speichern Sie die Änderungen, und schließen Sie die Datei.

7 Wechseln Sie in das Verzeichnis `/etc/security/`, und geben Sie folgenden Befehl ein, um eine Nulllängendatei mit dem Namen `opasswd` zu erstellen:

```
touch opasswd
```

8 Geben Sie die folgenden Befehle ein:

```
chmod 0600 opasswd
chown root:root /etc/security/opasswd
```

So ändern Sie Standardkomplexität von Kennwörtern für das Plug-In „pam_cracklib.so“

1 Melden Sie sich an der Servicekonsole an, und rufen Sie Root-Berechtigungen ab.

2 Geben Sie den folgenden Befehl ein:

```
esxcfg-auth --usecrack=<Wiederholungen> <Mindestlänge> <KB_Bonus>
<GB_Bonus> <Z_Bonus> <AZ_Bonus>
```

hierbei gilt:

- Der Wert für `Wiederholungen` gibt die Anzahl der zulässigen Wiederholungsversuche an, nach deren Überschreiten ESX Server 3 den Benutzer aus dem Kennwortänderungsmodus ausschließt.

- Die `Mindestlänge` ist die Mindestanzahl an Zeichen, die ein Benutzer eingeben muss, damit das Kennwort angenommen wird. Diese Anzahl ist die Gesamtlänge vor der Anwendung jeglicher Zeichenboni.

  Es wird immer mindestens ein Zeichenbonus angewendet. Daher ist die Kennwortlänge effektiv ein Zeichen kürzer als im Parameter `Mindestlänge` angegeben. Da das Plug-In `pam_cracklib.so` nur Kennwörter mit mindestens 6 Zeichen akzeptiert, muss der Parameter `Mindestlänge` so berechnet werden, dass die Kennwortlänge nach Abzug der Zeichenboni nicht kleiner als 6 sein kann.

- `KB_Bonus` ist die Anzahl an Zeichen, um die der Parameter `Mindestlänge` verringert wird, wenn im Kennwort mindestens ein Kleinbuchstabe enthalten ist.
- `GB_Bonus` ist die Anzahl an Zeichen, um die der Parameter `Mindestlänge` verringert wird, wenn im Kennwort mindestens ein Großbuchstabe enthalten ist.
- `Z_Bonus` ist die Anzahl an Zeichen, um die der Parameter `Mindestlänge` verringert wird, wenn im Kennwort mindestens eine Ziffer enthalten ist.
- `AZ_Bonus` ist die Anzahl der Zeichen, um die der Parameter `Mindestlänge` verringert wird, wenn der Benutzer mindestens ein Sonderzeichen wie z. B. einen Unterstrich oder einen Bindestrich verwendet.

Geben Sie die Zeichenbonusparameter als positive Zahl oder, wenn der Benutzer keinen Bonus für diese Zeichenklasse erhalten soll, als „0“ an. Die Zeichenboni werden addiert. Je mehr verschiedene Zeichenarten der Benutzer eingibt, desto weniger Zeichen sind notwendig, um ein gültiges Kennwort zu erstellen. Beispiel:

```
esxcfg-auth --usecrack=3 11 1 1 1 2
```

Mit dieser Einstellung benötigt ein Benutzer, der ein Kennwort aus Kleinbuchstaben und einem Unterstrich erstellt, acht Zeichen, um ein gültiges Kennwort zu erstellen. Wenn der Benutzer hingegen alle Zeichenarten (Kleinbuchstaben, Großbuchstaben, Zahlen und Sonderzeichen) einfügt, benötigt er nur sechs Zeichen.

Ändern des Kennwort-Plug-Ins

Für die meisten Umgebungen ist das Plug-In `pam_cracklib.so` zur Durchsetzung einer ordnungsgemäßen Kennwortqualität ausreichend. Wenn `pam_cracklib.so` jedoch nicht Ihren Bedürfnissen entspricht, können Sie auch das Plug-In `pam_passwdqc.so` verwenden. Sie können das Plug-In über den Befehl `esxcfg-auth` ändern.

Das Plug-In `pam_passwdqc.so` überprüft dieselben Kennwortmerkmale wie das Plug-In `pam_cracklib.so`. Es bietet jedoch mehr Optionen zur Feinabstimmung

der Kennwortqualität und führt für alle Benutzer einschließlich des Root-Benutzers Kennwortqualitätstests durch. Das Plug-In `pam_passwdqc.so` ist ferner etwas schwieriger in der Nutzung als das Plug-In `pam_cracklib.so`. Weitere Informationen zu diesem Plug-In finden Sie in der Linux-Dokumentation.

HINWEIS Das in Linux verwendete Plug-In `pam_passwdqc.so` bietet mehr Parameter als die Parameter, die von ESX Server 3 unterstützt werden. Sie können diese zusätzlichen Parameter nicht in `esxcfg-auth` angeben.

So wechseln zum Plug-In „pam_passwdqc.so“

1 Melden Sie sich an der Servicekonsole an, und rufen Sie Root-Berechtigungen ab.

2 Geben Sie den folgenden Befehl ein:

```
esxcfg-auth --usepamqc=<N0> <N1> <N2> <N3> <N4> <Übereinstimmung>
```

wobei:

- `N0` die Anzahl an Zeichen ist, die für ein Kennwort notwendig sind, das nur aus Zeichen einer Zeichenklasse gebildet wird.
- `N1` die Anzahl an Zeichen ist, die für ein Kennwort notwendig sind, das aus Zeichen von zwei Zeichenklassen gebildet wird.
- `N2` für Kennwortsätze verwendet wird. Für ESX Server 3 sind mindestens drei Wörter notwendig, um einen Kennwortsatz zu bilden.
- `N3` die Anzahl an Zeichen ist, die für ein Kennwort notwendig sind, das aus Zeichen von drei Zeichenklassen gebildet wird.
- `N4` die Anzahl an Zeichen ist, die für ein Kennwort notwendig sind, das aus Zeichen von allen vier Zeichenklassen gebildet wird.
- `Übereinstimmung` die Anzahl an Zeichen ist, die in einer Zeichenfolge wiederverwendet wird, die aus dem alten Kennwort stammt. Wenn `pam_passwdqc.so` eine wiederverwendete Zeichenfolge mit mindestens dieser Länge findet, schließt es diese Zeichenfolge aus dem Qualitätstest aus und verwendet zur Prüfung nur die übrigen Zeichen.

Wenn eine dieser Optionen auf `-1` gesetzt wird, ignoriert `pam_passwdqc.so` diese Anforderung. Wenn eine dieser Optionen auf `disabled` gesetzt wird, lehnt `pam_passwdqc.so` das Kennwort mit einem entsprechenden Merkmal ab. Die Werte müssen in absteigender Reihenfolge verwendet werden. Ausgenommen hiervon sind `-1` und `disabled`.

Beispiel:

```
esxcfg-auth --usepamqc=disabled 18 -1 12 8
```

In dieser Einstellung werden alle Kennwörter, die ein Benutzer erstellt und die nur eine Zeichenklasse enthalten, abgelehnt. Ein Kennwort mit zwei Zeichenklassen muss mindestens 18 Zeichen lang sein, ein Kennwort mit drei Zeichenklassen 12 Zeichen lang und ein Kennwort mit vier Zeichenklassen 8 Zeichen lang. Versuche zur Erstellung eines Kennwortsatzes werden ignoriert.

Schlüsselqualität

Die Übertragung von Daten über unsichere Verbindungen stellt ein Sicherheitsrisiko dar, da böswillige Benutzer Daten scannen können, während sie im Netzwerk übertragen werden. Als Schutz dagegen verschlüsseln die Netzwerkkomponenten meistens die Daten, sodass diese nicht so einfach gelesen werden können. Zur Verschlüsselung verwendet die sendende Komponente, zum Beispiel ein Gateway oder ein Redirector, Algorithmen, Algorithmen (sog. *Schlüssel*), um die Daten zu ändern, bevor sie übertragen werden. Die Zielkomponente verwendet dann einen Schlüssel, um die Daten zu entschlüsseln und sie in ihre ursprüngliche Form zu bringen.

Derzeit werden verschiedene Schlüssel verwendet. Die Sicherheitsebene jedes dieser Schlüssel ist unterschiedlich. Ein Maß zur Bestimmung der Datenschutzfähigkeit eines Schlüssels ist die *Schlüsselqualität*, d h. die Anzahl der Bits im Verschlüsselungsschlüssel. Je höher diese Anzahl ist, desto sicherer ist der Schlüssel.

Damit die Daten aus und zu externen Netzwerken gesendeten Daten geschützt werden, verwendet ESX Server 3 einen der sichersten Blockschlüssel, den es derzeit gibt, die 256-Bit-AES-Blockverschlüsselung. ESX Server 3 verwendet außerdem 1024-Bit-RSA für den Schlüsselaustausch. Diese Verschlüsselungsalgorithmen sind für folgende Verbindungen Standard:

- VI Client-Verbindungen zu VirtualCenter Server und zum ESX Server 3-Host über die Servicekonsole.
- VI Web Access-Verbindungen zum ESX Server 3-Host über die Servicekonsole.

  HINWEIS Da die Verwendung von Verschlüsselungstechniken für VI Web Access vom Web-Browser abhängig ist, den Sie verwenden, verwendet dieses Verwaltungsprogramm ggf. eine andere Verschlüsselung.

- SDK-Verbindungen zu VirtualCenter Server und zum ESX Server 3.
- Servicekonsolenverbindungen zu den virtuellen Maschinen über VMkernel.
- SSH-Verbindungen zum ESX Server 3-Host über die Servicekonsole. Weitere Informationen finden Sie unter „SSH-Sicherheit“ auf Seite 265.

setuid- und setgid-Anwendungen

`setuid` ist ein Kennzeichen, mit dem eine Anwendung die Zugriffsberechtigungen eines Benutzers, der die Anwendung ausführt, ändern kann, indem es die tatsächliche Benutzer-ID auf die Benutzer-ID des Programmbesitzers setzt. `setgid` ist ein Kennzeichen, mit dem eine Anwendung die Zugriffsberechtigungen einer Gruppe, die die Anwendung ausführt, ändern kann, indem es die tatsächliche Gruppen-ID auf die Gruppen-ID des Programmbesitzers setzt.

Während der Installation von ESX Server 3 werden standardmäßig verschiedene Anwendungen installiert, die das `setuid`- und `setgid`-Kennzeichen enthalten. Diese Anwendungen werden von der oder über die Servicekonsole aufgerufen. Manche dieser Anwendungen enthalten Hilfsprogramme, die zur korrekten Ausführung des ESX Server 3-Hosts notwendig sind. Andere Anwendungen sind optional, erleichtern aber ggf. die Wartung und Fehlerbehebung auf dem ESX Server 3-Host und im Netzwerk.

setuid-Standardanwendungen

Tabelle 12-3 listet die `setuid`-Standardanwendungen auf und zeigt an, ob eine Anwendung erforderlich oder optional ist.

Tabelle 12-3. setuid-Standardanwendungen

Anwendung	Zweck und Pfad	Erforderlich oder optional
`crontab`	Ermöglicht einzelnen Benutzern, Cron-Aufträge hinzuzufügen. **Pfad:** `/usr/bin/crontab`	Optional
`pam_timestamp_check`	Unterstützt Kennwortauthentifizierung. **Pfad:** `/sbin/pam_timestamp_check`	Erforderlich
`passwd`	Unterstützt Kennwortauthentifizierung. **Pfad:** `/usr/bin/passwd`	Erforderlich
`ping`	Sendet und wartet auf Kontrolldatenpakete an der Netzwerkschnittstelle. Nützlich zur Problemsuche in Netzwerken. **Pfad:** `/bin/ping`	Optional
`pwdb_chkpwd`	Unterstützt Kennwortauthentifizierung. **Pfad:** `/sbin/pwdb_chkpwd`	Erforderlich

Tabelle 12-3. setuid-Standardanwendungen (Fortsetzung)

Anwendung	Zweck und Pfad	Erforderlich oder optional
`ssh-keysign`	Zur hostbasierten Authentifizierung für SSH. **Pfad:** `/usr/libexec/openssh/ssh-keysign`	Erforderlich, wenn Sie eine hostbasierte Authentifizierung verwenden. Ansonsten optional.
`su`	Macht durch Benutzerwechsel aus einem allgemeinen Benutzer einen Root-Benutzer. **Pfad:** `/bin/su`	Erforderlich
`sudo`	Macht aus einem allgemeinen Benutzer für bestimmte Vorgänge einen Root-Benutzer. **Pfad:** `/usr/bin/sudo`	Optional
`unix_chkpwd`	Unterstützt Kennwortauthentifizierung. **Pfad:** `/sbin/unix_chkpwd`	Erforderlich
`vmkload_app`	Führt Aufgaben zur Ausführung virtueller Maschinen aus. Diese Anwendung befindet sich an zwei Speicherorten: an einem Speicherort zur normalen Verwendung und an einem zur Fehlersuche. **Pfad für normale Verwendung:** `/usr/lib/vmware/bin/vmkload_app` **Pfad zur Fehlersuche:** `/usr/lib/vmware/bin-debug/vmkload_app`	In beiden Verzeichnissen erforderlich
`vmware-authd`	Authentifiziert Benutzer zur Verwendung bestimmter VMware-Dienste. **Pfad:** `/usr/sbin/vmware-authd`	Erforderlich
`vmware-vmx`	Führt Aufgaben zur Ausführung virtueller Maschinen aus. Diese Anwendung befindet sich an zwei Speicherorten: an einem Speicherort zur normalen Verwendung und an einem zur Fehlersuche. **Pfad für normale Verwendung:** `/usr/lib/vmware/bin/vmware-vmx` **Pfad zur Fehlersuche:** `/usr/lib/vmware/bin-debug/vmware-vmk`	In beiden Verzeichnissen erforderlich

Wenn Sie eine der erforderlichen Anwendungen deaktivieren, führt dies zu Problemen bei der ESX Server 3-Authentifizierung und beim Betrieb der virtuellen Maschinen. Sie können jedoch alle optionalen Anwendungen deaktivieren.

So deaktivieren Sie eine optionale setuid-Anwendung

1 Melden Sie sich an der Servicekonsole an, und rufen Sie Root-Berechtigungen ab.

2 Führen Sie den folgenden Befehl aus:

```
chmod a-s <Pfad zur ausführbaren Datei>
```

setgid-Standardanwendungen

Es werden standardmäßig zwei Anwendungen installiert, die das `setgid`-Kennzeichen enthalten. Tabelle 12-4 listet die `setgid`-Standardanwendungen auf und zeigt an, ob eine Anwendung erforderlich oder optional ist.

Tabelle 12-4. `setgid`-Standardanwendungen

Anwendung	Zweck und Pfad	Erforderlich oder optional
`wall`	Warnt alle Anschlüsse, dass ein bestimmter Vorgang bevorsteht. Diese Anwendung wird durch `shutdown` und andere Befehle aufgerufen. **Pfad:** `/usr/bin/wall`	Optional
`lockfile`	Führt Sperroperationen für den Dell OM-Management-Agenten aus. **Pfad:** `/usr/bin/lockfile`	Für Dell OM erforderlich, ansonsten optional

Wenn Sie eine der erforderlichen Anwendungen deaktivieren, führt dies zu Problemen bei der ESX Server 3-Authentifizierung und beim Betrieb der virtuellen Maschinen. Sie können jedoch alle optionalen Anwendungen deaktivieren.

So deaktivieren Sie eine optionale setgid-Anwendung

1 Melden Sie sich an der Servicekonsole an, und rufen Sie Root-Berechtigungen ab.

2 Führen Sie den folgenden Befehl aus:

```
chmod a-s <Pfad zur ausführbaren Datei>
```

SSH-Sicherheit

SSH ist eine häufig verwendete UNIX- und Linux-Befehlsshell, mit der Sie sich aus der Ferne auf der Servicekonsole anmelden und bestimmte Management- und Konfigurationsaufgaben für ESX Server durchführen können. SSH wird für sichere Anmeldevorgänge und Datenübertragungen verwendet, weil es einen höheren Schutz als andere Befehlsshells bietet. In dieser ESX Server 3-Version wurde die

SSH-Konfiguration verbessert, um eine noch höhere Sicherheit zu gewährleisten. Zu diesen Verbesserungen gehören unter anderem:

- **Deaktivierung des SSH-Protokolls, Version 1** – VMware unterstützt das SSH-Protokoll in Version 1 nicht mehr, sondern verwendet nun ausschließlich das Protokoll in Version 2. Version 2 behebt bestimmte Sicherheitsprobleme von Version 1 und bietet eine sicherere Kommunikationsschnittstelle zur Servicekonsole.
- **Verbesserte Schlüsselqualität** – SSH unterstützt nun nur noch 256-Bit- und 128-Bit-AES-Schlüssel für Verbindungen.
- **Beschränkte Fernanmeldung als Root** – Eine Remoteanmeldung als Root-Benutzer ist nicht mehr möglich. Sie melden sich stattdessen als Benutzer an und verwenden dann entweder den Befehl `sudo`, um bestimmte Vorgänge, die Root-Berechtigungen erfordern, auszuführen, oder den Befehl `su`, um zum Root-Benutzer zu werden.

  HINWEIS Der Befehl `sudo` bietet Sicherheitsvorteile, da er die Root-Aktivitäten einschränkt und ermöglicht, den möglichen Missbrauch von Root-Berechtigungen zu überprüfen, indem er eine Prüfliste alle Root-Aktivitäten anlegt, die der Benutzer durchführt.

Diese Einstellungen wurden so entworfen, dass die Daten, die Sie über SSH an die Servicekonsole übertragen, gut geschützt werden. Wenn diese Konfiguration für Ihre Bedürfnisse zu streng ist, können Sie die Sicherheitsparameter senken.

So ändern Sie die SSH-Standardkonfiguration

1. Melden Sie sich an der Servicekonsole an, und rufen Sie Root-Berechtigungen ab.
2. Wechseln Sie in der Eingabeaufforderung über den Befehl **`cd /etc/ssh`** das Verzeichnis.
3. Führen Sie in einem Texteditor nach Bedarf einen oder mehrere der folgenden Vorgänge aus.
   - Wenn Sie die Root-Remote-Anmeldung zulassen möchten, ändern Sie die Einstellung in der folgenden Zeile der Datei `sshd_config` in `yes`:

     ```
     PermitRootLogin no
     ```
   - Um zum ursprünglichen SSH-Protokoll (Version 1 und 2) zurückzukehren, kommentieren Sie folgende Zeile in der Datei `sshd_config` aus:

     ```
     Protocol 2
     ```

- Um 3DES-Verschlüsselung und andere Verschlüsselungsarten auch weiterhin zu verwenden, kommentieren Sie folgende Zeile in der Datei `sshd_config` aus:

  ```
  Ciphers aes256-cbc,aes128-cbc
  ```

- Um Secure FTP (SFTP) auf SSH zu deaktivieren, kommentieren Sie folgende Zeile in der Datei `sshd_config` aus:

  ```
  Subsystem ftp /usr/libexec/openssh/sftp-server
  ```

4 Speichern Sie die Änderungen, und schließen Sie die Datei.

5 Geben Sie folgenden Befehl ein, um den SSHD-Dienst neu zu starten:

```
service sshd restart
```

Sicherheitspatches und Software zum Suchen nach Sicherheitslücken

Wenn ein Patch für ein bestimmtes von LINUX unterstütztes Softwarepaket, das von VMware als Servicekonsolenkomponente angeboten wird, zum Beispiel ein Dienst, ein Hilfsprogramm oder ein Protokoll, verfügbar wird, stellt VMware ein Paket für den RPM Package Manager (RPM) zur Verfügung, mit dem Sie das Softwarepaket auf ESX Server 3 aktualisieren können. Verwenden Sie immer die RPMs, die VMware zur Verfügung stellt, selbst wenn diese Patches auch von Drittanbietern als RPM angeboten werden.

Bei der Veröffentlichung von Patches für ein Softwarepaket portiert VMware den Patch grundsätzlich auf eine Version der Software zurück, die auch wirklich stabil ist. Durch diese Herangehensweise werden die Chancen verringert, dass durch den Patch neue Fehler und Stabilitätsprobleme in die Software gelangen. Da der Patch auf eine bestehende Version der Software aufgespielt wird, bleibt die Versionsnummer der Software gleich, nur die Patchnummer wird als Suffix angehängt.

Bestimmte Sicherheitssuchprogramme wie Nessus überprüfen zwar die Versionsnummer, nicht jedoch das Patch-Suffix, wenn sie nach Sicherheitslücken suchen. Daher kann es dazu kommen, dass diese Suchprogramme fälschlicherweise melden, dass die Software nicht aktuell ist und – ungeachtet der Realität – nicht die neuesten Sicherheitspatches enthält. Dieses Problem tritt in der IT-Branche häufig auf und ist nicht auf VMware beschränkt.

HINWEIS Einige Sicherheitssuchprogramme sind in der Lage, diese Situation ordnungsgemäß abzuhandeln, aber normalerweise liegen sie um eine Version oder mehr zurück. So meldet die Nessus-Version, die nach einem Red Hat-Patch veröffentlicht wird, diese Fehlmeldungen meistens nicht.

Es folgt ein Beispiel, wie dieses Problem entsteht:

1 Sie installieren ESX Server 3 mit OpenSSL, Version 0.9.7a (wobei 0.9.7a die ursprüngliche Version ohne Patches ist).

2 OpenSSL veröffentlicht einen Patch, der eine Sicherheitslücke in Version 0.9.7 schließt. Diese Version wird 0.9.7x genannt.

3 VMware portiert den Patch OpenSSL 0.9.7x auf die ursprüngliche Version zurück, aktualisiert die Patchnummer und erstellt ein RPM. Die OpenSSL-Version in dem RPM ist 0.9.7a-1, d. h. die ursprüngliche Version (0.9.7a) enthält nun Patch 1.

4 Sie installieren den RPM.

5 Das Sicherheitssuchprogramm übersieht das Suffix „-1“ und meldet fälschlicherweise, dass die Sicherheitseinstellungen für OpenSSL nicht aktuell sind.

Wenn Ihr Suchprogramm meldet, dass die Sicherheitseinstellungen für ein Paket nicht aktuell sind, führen Sie die folgenden Überprüfungen durch:

- Überprüfen Sie das Patch-Suffix, um zu bestimmen, ob Sie eine Aktualisierung benötigen.
- Konsultieren Sie die RPM-Dokumentation von VMware bezüglich Informationen zu den Patchinhalten.
- Verwenden Sie folgenden Befehl, um die „Common Vulnerabilities and Exposures” -Nummer (CVE) aus der Sicherheitswarnung im RPM-Änderungsprotokoll nachzuschlagen:

  ```
  rpm–q ––changelog openssl | grep <CVE_Nummer>
  ```

  Wenn sich die CVE-Nummer dort befindet, deckt das Paket die Sicherheitslücke ab.

Empfehlungen für den Schutz von Implementierungen

13

Dieses Kapitel soll Ihnen eine bessere Vorstellung von der Absicherung von ESX Server 3 in bestimmten Umgebungen vermitteln. Dazu wird eine Reihe von ESX Server 3-Implementierungsszenarien vorgestellt, die Ihnen bei der Planung der Sicherheitsfunktionen in Ihrer eigenen Implementierung helfen können. Außerdem enthält dieses Kapitel einige grundlegende Sicherheitsempfehlungen, die Sie bei der Erstellung und Konfiguration virtueller Maschinen in Betracht ziehen sollten.

In diesem Kapitel werden folgende Themen behandelt:

- „Sicherheitsmaßnahmen für gängige ESX Server 3-Implementierungen“ auf Seite 269
- „Empfehlungen für virtuelle Maschinen“ auf Seite 276

Sicherheitsmaßnahmen für gängige ESX Server 3-Implementierungen

Die Komplexität von ESX Server 3-Implementierungen kann je nach Größe Ihres Unternehmens, der gemeinsamen Nutzung von Daten und Ressourcen durch externe Parteien und der Verwendung eines oder mehrerer Datencenter usw. variieren.

Zu den folgenden Implementierungen gehören Richtlinien für den Benutzerzugriff, die gemeinsame Nutzung von Ressourcen sowie Sicherheitsstufen. Durch den Vergleich der Implementierungen können Sie die Probleme erkennen, die Sie bei der Planung der Sicherheit für Ihre eigene ESX Server 3-Implementierung beachten müssen.

Implementierung „für einen Kunden“

Bei dieser Implementierung befinden sich die ESX Server 3-Hosts in einem Unternehmen und einem einzelnen Datencenter und werden auch dort verwaltet. ESX Server 3-Ressourcen werden nicht durch externe Benutzer genutzt. Die ESX Server 3-Hosts werden von einem globalen Administrator verwaltet, und auf den Hosts werden mehrere virtuelle Maschinen ausgeführt.

Die Implementierung lässt Kundenadministratoren nicht zu, und der Standortadministrator ist allein für die Verwaltung der verschiedenen virtuellen Maschinen verantwortlich. Das Unternehmen beschäftigt mehrere Systemadministratoren, die keine Konten auf dem ESX Server 3-Host haben und nicht auf ESX Server 3-Programme wie VirtualCenter oder Befehlszeilenshells für den Host zugreifen können. Diese Systemadministratoren haben über die VM-Konsole Zugriff auf die virtuellen Maschinen, sodass Sie Software installieren und andere Verwaltungsaufgaben in den virtuellen Maschinen durchführen können.

Tabelle 13-1 zeigt, wie Sie die Komponenten gemeinsam nutzen und für den ESX Server 3-Host konfigurieren können.

Tabelle 13-1. Gemeinsame Komponentennutzung bei einer Implementierung für einen Kunden

Funktion	Konfiguration	Anmerkungen
Servicekonsole im gleichen physischen Netzwerk wie die virtuellen Maschinen?	Nein	Isolieren Sie die Servicekonsole, sodass sie über ihr eigenes physisches Netzwerk verfügt.
Servicekonsole im gleichen VLAN wie die virtuellen Maschinen?	Nein	Isolieren Sie die Servicekonsole, sodass sie über ihr eigenes VLAN verfügt. Virtuelle Maschinen oder andere Systemkomponenten, z. B. VMotion, sollten ein anderes VLAN verwenden.
Virtuelle Maschinen im gleichen physischen Netzwerk?	Ja	Die virtuellen Maschinen nutzen das gleiche physische Netzwerk.
Gemeinsame Netzwerkadapternutzung?	Teilweise	Isolieren Sie die Servicekonsole, sodass sie über ihren eigenen virtuellen Switch und virtuellen Netzwerkadapter verfügt. Virtuelle Maschinen oder andere Systemkomponenten sollten einen anderen Switch oder Adapter verwenden. Die virtuellen Maschinen können sich jedoch einen virtuellen Switch oder Netzwerkadapter teilen.
Gemeinsame VMFS-Nutzung?	Ja	Alle `.vmdk`-Dateien sollten sich in der gleichen VMFS-Partition befinden.

Tabelle 13-1. Gemeinsame Komponentennutzung bei einer Implementierung für einen Kunden (Fortsetzung)

Funktion	Konfiguration	Anmerkungen
Sicherheitsstufe	Hoch	Geben Sie Ports für benötigte Dienste wie FTP nach Bedarf frei. Weitere Informationen zu den Sicherheitsstufen finden Sie unter „Konfiguration der Servicekonsolen-Firewall“ auf Seite 249.
Speichermehrfachvergabe für virtuelle Maschinen?	Ja	Der konfigurierte Gesamtspeicher für die virtuellen Maschinen kann größer als der physische Gesamtspeicher sein.

Tabelle 13-2 zeigt, wie die Benutzerkonten für den ESX Server 3-Host eingerichtet werden können.

Tabelle 13-2. Benutzerkonten bei einer Implementierung für einen Kunden

Benutzerkategorie	Gesamtanzahl an Konten
Standortadministratoren	1
Kundenadministratoren	0
Systemadministratoren	0
Unternehmensbenutzer	0

Tabelle 13-3 Die folgende Tabelle zeigt die Zugriffsberechtigungen für die Benutzer.

Tabelle 13-3. Benutzerzugriff in einer Implementierung für einen Kunden

Zugriffsumfang	Standortadministrator	Systemadministrator
Root-Zugriff?	Ja	Nein
Servicekonsolenzugriff über SSH?	Ja	Nein
VirtualCenter und VI Web Access?	Ja	Nein
Erstellung und Änderung virtueller Maschinen?	Ja	Nein
Zugriff auf virtuelle Maschinen über die Konsole?	Ja	Ja

Eingeschränkte Implementierung für mehrere Kunden

In dieser Implementierung befinden sich die ESX Server 3-Hosts im gleichen Datencenter und werden für Anwendungen mehrerer Kunden verwendet. Der Standortadministrator verwaltet die ESX Server 3-Hosts, auf denen mehrere virtuelle Maschinen jeweils für die einzelnen Kunden ausgeführt werden. Die virtuellen Maschinen der verschiedenen Kunden können sich auf dem gleichen ESX Server 3-Host befinden, doch der Standortadministrator beschränkt die gemeinsame Nutzung von Ressourcen, um die Datensicherheit zu gewährleisten.

Es gibt einen Standortadministrator und mehrere Kundenadministratoren, die die virtuellen Maschinen ihrer jeweiligen Kunden verwalten. Zu dieser Implementierung gehören auch Systemadministratoren der Kunden, die kein ESX Server 3-Konto haben, doch über die VM-Konsole auf die virtuellen Maschinen zugreifen können, um Software zu installieren und andere Verwaltungsaufgaben in den virtuellen Maschinen durchzuführen.

Tabelle 13-4 zeigt, wie Sie die Komponenten gemeinsam nutzen und für den ESX Server 3-Host konfigurieren können.

Tabelle 13-4. Gemeinsame Komponentennutzung in einer beschränkten Implementierung für mehrere Kunden

Funktion	Konfiguration	Anmerkungen
Servicekonsole im gleichen physischen Netzwerk wie die virtuellen Maschinen?	Nein	Isolieren Sie die Servicekonsole, sodass sie über ihr eigenes physisches Netzwerk verfügt.
Servicekonsole im gleichen VLAN wie die virtuellen Maschinen?	Nein	Isolieren Sie die Servicekonsole, sodass sie über ihr eigenes VLAN verfügt. Virtuelle Maschinen oder andere Systemkomponenten, z. B. VMotion, sollten ein anderes VLAN verwenden.
Virtuelle Maschinen im gleichen physischen Netzwerk?	Teilweise	Installieren Sie die virtuellen Maschinen jedes Kunden in einem anderen physischen Netzwerk. Alle physischen Netzwerke sind voneinander unabhängig.

Tabelle 13-4. Gemeinsame Komponentennutzung in einer beschränkten Implementierung für mehrere Kunden (Fortsetzung)

Funktion	Konfiguration	Anmerkungen
Gemeinsame Netzwerkadapternutzung?	Teilweise	Isolieren Sie die Servicekonsole, sodass sie über ihren eigenen virtuellen Switch und virtuellen Netzwerkadapter verfügt. Virtuelle Maschinen oder andere Systemkomponenten sollten einen anderen Switch oder Adapter verwenden. Die virtuellen Maschinen eines Kunden können den gleichen virtuellen Switch und Netzwerkadapter haben. Sie sollten sich jedoch Switch und Adapter nicht mit anderen Kunden teilen.
Gemeinsame VMFS-Nutzung?	Nein	Jeder Kunde hat seine eigene VMFS-Partition, die `.vmdk`-Dateien der virtuellen Maschinen befinden sich ausschließlich auf dieser Partition. Die Partition kann mehrere LUNs umfassen.
Sicherheitsstufe	Hoch	Geben Sie Ports für Dienste wie FTP nach Bedarf frei.
Speichermehrfachvergabe für virtuelle Maschinen?	Ja	Der konfigurierte Gesamtspeicher für die virtuellen Maschinen kann größer als der physische Gesamtspeicher sein.

Tabelle 13-5 zeigt, wie die Benutzerkonten für den ESX Server 3-Host eingerichtet werden können.

Tabelle 13-5. Benutzerkonten in einer Implementierung für einen Kunden

Benutzerkategorie	Gesamtanzahl an Konten
Standortadministratoren	1
Kundenadministratoren	10
Systemadministratoren	0
Unternehmensbenutzer	0

Tabelle 13-6 Die folgende Tabelle zeigt die Zugriffsberechtigungen für die Benutzer.

Tabelle 13-6. Benutzerzugriff in einer beschränkten Implementierung für mehrere Kunden

Zugriffsumfang	Standort-administrator	Kunden-administrator	System-administrator
Root-Zugriff?	Ja	Nein	Nein
Servicekonsolenzugriff über SSH?	Ja	Ja	Nein
VirtualCenter und VI Web Access?	Ja	Ja	Nein
Erstellung und Änderung virtueller Maschinen?	Ja	Ja	Nein
Zugriff auf virtuelle Maschinen über die Konsole?	Ja	Ja	Ja

Beschränkte Implementierung für mehrere Kunden

Bei dieser Implementierung befinden sich die ESX Server 3-Hosts im gleichen Datencenter und werden für Anwendungen mehrerer Kunden verwendet. Der Standortadministrator verwaltet die ESX Server 3-Hosts, auf denen mehrere virtuelle Maschinen jeweils für die einzelnen Kunden ausgeführt werden. Die virtuellen Maschinen der verschiedenen Kunden können sich auf dem gleichen ESX Server 3-Host befinden, doch es gibt weniger Beschränkungen zur gemeinsamen Nutzung von Ressourcen.

Es gibt einen Standortadministrator und mehrere Kundenadministratoren, die die virtuellen Maschinen ihrer jeweiligen Kunden verwalten. Zu dieser Implementierung gehören auch Systemadministratoren der Kunden, die kein ESX Server 3-Konto haben, doch über die VM-Konsole auf die virtuellen Maschinen zugreifen können, um Software zu installieren und andere Verwaltungsaufgaben in den virtuellen Maschinen durchzuführen. Außerdem kann eine Gruppe von Unternehmensbenutzern ohne Konten die virtuellen Maschinen zur Ausführung ihrer Anwendungen verwenden.

Tabelle 13-7 zeigt, wie Sie die Komponenten gemeinsam nutzen und für den ESX Server 3-Host konfigurieren können.

Tabelle 13-7. Gemeinsame Komponentennutzung in einer unbeschränkten Implementierung für mehrere Kunden

Funktion	Konfiguration	Anmerkungen
Servicekonsole im gleichen physischen Netzwerk wie die virtuellen Maschinen?	Nein	Isolieren Sie die Servicekonsole, sodass sie über ihr eigenes physisches Netzwerk verfügt.
Servicekonsole im gleichen VLAN wie die virtuellen Maschinen?	Nein	Isolieren Sie die Servicekonsole, sodass sie über ihr eigenes VLAN verfügt. Virtuelle Maschinen oder andere Systemkomponenten, z. B. VMotion, sollten ein anderes VLAN verwenden.
Virtuelle Maschinen im gleichen physischen Netzwerk?	Ja	Die virtuellen Maschinen nutzen das gleiche physische Netzwerk.
Gemeinsame Netzwerkadapternutzung?	Teilweise	Isolieren Sie die Servicekonsole, sodass sie über ihren eigenen virtuellen Switch und virtuellen Netzwerkadapter verfügt. Virtuelle Maschinen oder andere Systemkomponenten sollten einen anderen Switch oder Adapter verwenden. Alle virtuellen Maschinen können sich einen virtuellen Switch oder Netzwerkadapter teilen.
Gemeinsame VMFS-Nutzung?	Ja	Die virtuellen Maschinen können VMFS-Partitionen gemeinsam nutzen, die `.vmdk`-Dateien der virtuellen Maschinen können sich auf einer gemeinsamen Partition befinden. Die virtuellen Maschinen verwenden keine gemeinsamen `.vmdk`-Dateien.
Sicherheitsstufe	Hoch	Geben Sie Ports für Dienste wie FTP nach Bedarf frei.
Speichermehrfachvergabe für virtuelle Maschinen?	Ja	Der konfigurierte Gesamtspeicher für die virtuellen Maschinen kann größer als der physische Gesamtspeicher sein.

Tabelle 13-8 zeigt, wie die Benutzerkonten für den ESX Server 3-Host eingerichtet werden können.

Tabelle 13-8. Benutzerkonten in einer Implementierung für einen Kunden

Benutzerkategorie	Gesamtanzahl an Konten
Standortadministratoren	1
Kundenadministratoren	10
Systemadministratoren	0
Unternehmensbenutzer	0

Tabelle 13-9 Die folgende Tabelle zeigt die Zugriffsberechtigungen für die Benutzer.

Tabelle 13-9. Benutzerzugriff in einer unbeschränkten Implementierung für mehrere Kunden

Zugriffsumfang	Standort-administrator	Kunden-administrator	System-administrator	Unternehmens-benutzer
Root-Zugriff?	Ja	Nein	Nein	Nein
Servicekonsolenzugriff über SSH?	Ja	Ja	Nein	Nein
VirtualCenter und VI Web Access?	Ja	Ja	Nein	Nein
Erstellung und Änderung virtueller Maschinen?	Ja	Ja	Nein	Nein
Zugriff auf virtuelle Maschinen über die Konsole?	Ja	Ja	Ja	Ja

Empfehlungen für virtuelle Maschinen

Ergreifen Sie bei der Überprüfung der Sicherheit virtueller Maschinen und ihrer Verwaltung folgende Sicherheitsmaßnahmen.

Installieren von Antivirensoftware

Da auf jeder virtuellen Maschine ein Standardbetriebssystem ausgeführt wird, sollten Sie es durch die Installation von Antivirensoftware gegen Viren schützen. Je nach Verwendungszweck der virtuellen Maschine sollte ggf. auch eine Firewall installiert werden.

HINWEIS Softwarefirewalls und Antivirensoftware können die Virtualisierungsleistung beeinflussen. Wenn Sie sich sicher sind, dass sich die virtuellen Maschinen in einer vollständig vertrauenswürdigen Umgebung befinden, können Sie diese beiden Sicherheitsmaßnahmen gegen Leistungsvorteile abwägen.

Deaktivieren von Kopier- und Einfügevorgängen zwischen Gastbetriebssystem und Remotekonsole

Wenn VMware Tools auf einer virtuellen Maschine ausgeführt wird, können Sie Kopier- und Einfügevorgänge zwischen dem Gastbetriebssystem und der Remotekonsole ausführen. Sobald das Konsolenfenster den Eingabefokus hat, können unbefugte Benutzer und Prozesse in der virtuellen Maschine auf die Zwischenablage der Konsole der virtuellen Maschine zugreifen. Wenn ein Benutzer vor der Verwendung der Konsole vertrauliche Informationen in die Zwischenablage kopiert, macht der Benutzer der virtuellen Maschine, ggf. unwissentlich, vertrauliche Daten zugänglich.

Um dies zu verhindern, können Sie Kopier- und Einfügevorgänge für das Gastbetriebssystem deaktivieren.

So deaktivieren Sie Kopier- und Einfügevorgänge zwischen Gastbetriebssystem und Remotekonsole

1 Melden Sie sich am VI-Client an, und wählen Sie die virtuelle Maschine in der Bestandsliste aus.

   Die Konfiguration für diese virtuelle Maschine wird auf der Registerkarte **Übersicht (Summary)** angezeigt.

2 Klicken Sie auf **Einstellungen bearbeiten (Edit Settings)**.

3 Klicken Sie auf **Optionen (Options)** > **Erweitert (Advanced)** > **Konfigurationsparameter (Configuration Parameters)**. Das Dialogfeld **Konfigurationsparameter (Configuration Parameters)** wird geöffnet.

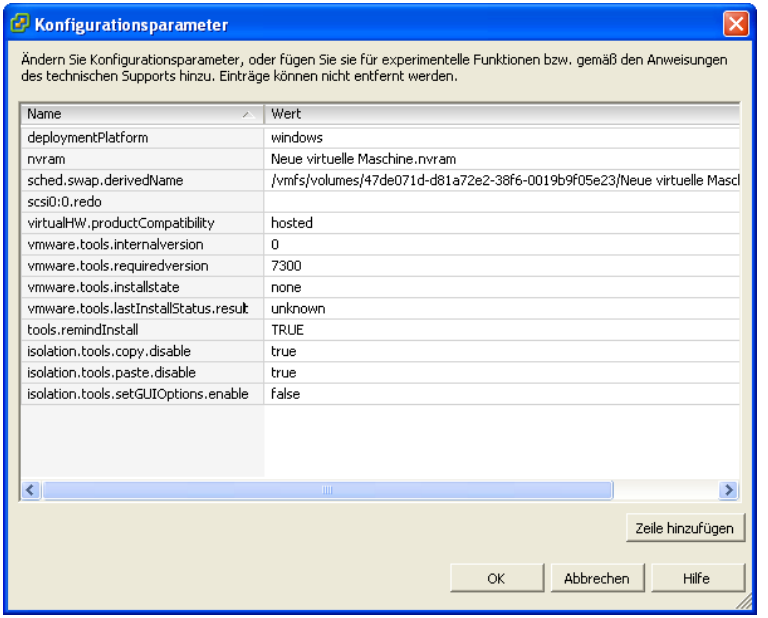
4 Klicken Sie auf die Schaltfläche **Hinzufügen (Add)**.

5 Geben Sie in der Spalte **Wert (Value)** für **Name** folgende Werte ein.

Tabelle 13-10. Konfigurationsparametereinstellungen

Feld „Name“	Feld „Wert“
`isolation.tools.copy.disable`	`true`
`isolation.tools.paste.disable`	`true`
`isolation.tools.setGUIOptions.enable`	`false`

Das Ergebnis sieht folgendermaßen aus.



HINWEIS Diese Optionen heben die Einstellungen in der Systemsteuerung von VMware Tools auf dem Gastbetriebssystem auf.

6 Klicken Sie auf **OK**, um das Dialogfeld **Konfigurationsparameter (Configuration Parameters)** zu schließen, und dann noch einmal auf **OK**, um das Dialogfeld **Eigenschaften der virtuellen Maschinen (Virtual Machine Properties)** zu schließen.

Entfernung überflüssiger Hardwaregeräte

Benutzer und Prozesse ohne Berechtigungen für die virtuelle Maschine können Hardwaregeräte wie Netzwerkadapter oder CD-ROM-Laufwerke einbinden oder trennen. Angreifer können diese Fähigkeit auf verschiedene Arten nutzen, um die Sicherheit einer virtuellen Maschine zu gefährden. So kann zum Beispiel ein Angreifer mit Zugang zu einer virtuellen Maschine folgende Angriffe durchführen:

- Einbinden eines nicht verbundenen CD-ROM-Laufwerks und Zugriff auf Informationen auf dem Medium, das sich im Laufwerk befindet.
- Trennen eines Netzwerkadapters, um die virtuelle Maschine vom Netzwerk zu isolieren, was zu einem Ausfall führt.

Als allgemeine Sicherheitsmaßnahme sollten Sie Befehle auf der Registerkarte **Konfiguration (Configuration)** auf dem VI-Client verwenden, um alle nicht benötigten oder ungenutzten Hardwaregeräte zu entfernen. Zwar erhöht diese Maßnahme die Sicherheit der virtuellen Maschinen, aber sie ist keine gute Lösung, wenn ein gegenwärtig ungenutztes Gerät später reaktiviert werden soll.

Wenn Sie ein Gerät nicht dauerhaft entfernen möchten, können Sie verhindern, dass ein Benutzer oder Prozess einer virtuellen Maschine das Gerät aus dem Gastbetriebssystem heraus einbindet oder trennt.

So hindern Sie einen Benutzer oder Prozess auf einer virtuellen Maschine am Trennen von Geräten

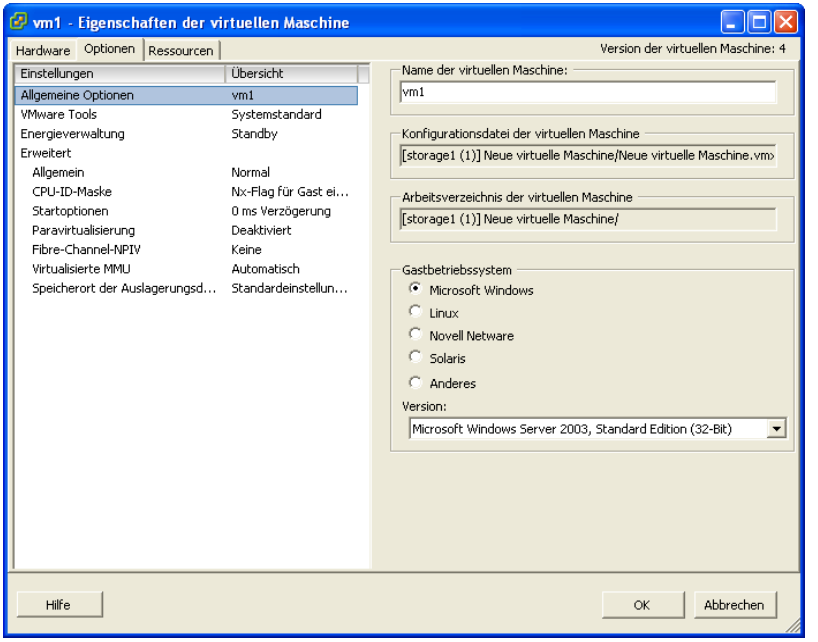
1 Melden Sie sich am VI-Client an, und wählen Sie die virtuelle Maschine in der Bestandsliste aus.

Die Konfiguration für diese virtuelle Maschine wird auf der Registerkarte **Übersicht (Summary)** angezeigt.

2 Klicken Sie auf **Einstellungen bearbeiten (Edit Settings)**.

Das Dialogfeld **Eigenschaften der virtuellen Maschine (Virtual Machine Properties)** wird geöffnet.

3 Klicken Sie auf **Optionen (Options)** > **Allgemein (General)**, und notieren Sie sich den Pfad, der im Feld **Konfigurationsdatei der virtuellen Maschine (Virtual Machine Configuration File)** angezeigt wird.



4 Melden Sie sich an der Servicekonsole an, und rufen Sie Root-Berechtigungen ab.

5 Wechseln Sie in das Verzeichnis, um auf die Konfigurationsdatei der virtuellen Maschine zuzugreifen, deren Pfad Sie sich in Schritt Schritt 3 notiert haben.

Die Konfigurationsdateien der virtuellen Maschinen befinden sich im Verzeichnis `/vmfs/volumes/<Datenspeicher>`, wobei es sich beim `<Datenspeicher>` um den Namen des Speichergeräts handelt, auf dem die Dateien der virtuellen Maschine gespeichert sind. Wenn beispielsweise die Konfigurationsdatei der virtuellen Maschine, die Sie im Dialogfeld **Eigenschaften der virtuellen Maschine (Virtual Machine Properties)** abgerufen haben, `[vol1]vm–finance/vm–finance.vmx` ist, wechseln Sie die Verzeichnisse wie folgt:

```
cd /vmfs/volumes/vol1/vm–finance/
```

6 Verwenden Sie Nano oder einen anderen Text-Editor, um die `.vmx`-Datei um die folgende Zeile zu ergänzen.

```
<Gerätename>.allowGuestConnectionControl = "false"
```

Wobei `<Gerätename>` der Name des Geräts ist, das geschützt werden soll, z. B. „ethernet1“.

HINWEIS Standardmäßig ist Ethernet 0 so konfiguriert, dass die Trennung des Geräts nicht möglich ist. Der einzige Grund, aus dem Sie veranlasst sein können, dies zu ändern, ergibt sich dann, wenn ein vorheriger Administrator `<Gerätename>.allowGuestConnectionControl` auf `true` gesetzt hat.

---

7 Speichern Sie die Änderungen, und schließen Sie die Datei.

8 Kehren Sie zum VI-Client zurück, und schalten Sie die virtuelle Maschine erst aus und dann wieder an. Dazu klicken Sie mit der rechten Maustaste auf die virtuelle Maschine im Bestandslistenfenster und klicken auf **Ausschalten (Power Off)** und anschließend auf **Einschalten (Power On)**.

Beschränken von Schreibvorgängen des Gastbetriebssystems in den Hostspeicher

Die Prozesse des Gastbetriebssystems senden über VMware Tools Informationsmeldungen an den ESX Server 3-Host. Diese Meldungen, die `setinfo`-Meldungen genannt werden, enthalten normalerweise Name/Wert-Paare zu Merkmalen virtueller Maschinen oder Bezeichner, die der Host speichert, zum Beispiel `ipaddress=10.17.87.224`.

Wenn die Datenmenge, die als Folge dieser Meldungen auf dem Host gespeichert wird, unbegrenzt wäre, würde eine unbeschränkte Datenübertragung einem Angreifer eine Gelegenheit zum Starten eines DoS-Angriffs (Denial of Service) bieten. Dazu müsste Code geschrieben werden, der VMware Tools imitiert und den Speicher des Hosts mit willkürlichen Konfigurationsdaten auffüllt, wodurch Speicherplatz belegt wird, der von den virtuellen Maschinen benötigt wird.

Um dies zu vermeiden, ist die Konfigurationsdatei mit diesen Name/Wert-Paaren auf eine maximale Größe von 1 MB beschränkt. 1 MB sollte in den meisten Fällen ausreichen. Sie können diesen Wert jedoch bei Bedarf ändern. Sie können beispielsweise diesen Wert erhöhen, wenn große Mengen von Kundendaten in der Konfigurationsdatei gespeichert werden.

Um das Speicherlimit von **GuestInfo** zu ändern, legen Sie das Attribut **tools.setInfo.sizeLimit** in der **.vmx (vmx)**-Datei fest. Das Standardlimit ist 1 MB, welches auch gilt, wenn das Attribut `sizeLimit` nicht vorhanden ist.

So ändern Sie das variable Speicherlimit des Gastbetriebssystems

1 Melden Sie sich am VI-Client an, und wählen Sie die virtuelle Maschine in der Bestandsliste aus.

   Die Konfiguration für diese virtuelle Maschine wird auf der Registerkarte **Übersicht (Summary)** angezeigt.

2 Klicken Sie auf **Einstellungen bearbeiten (Edit Settings)**.

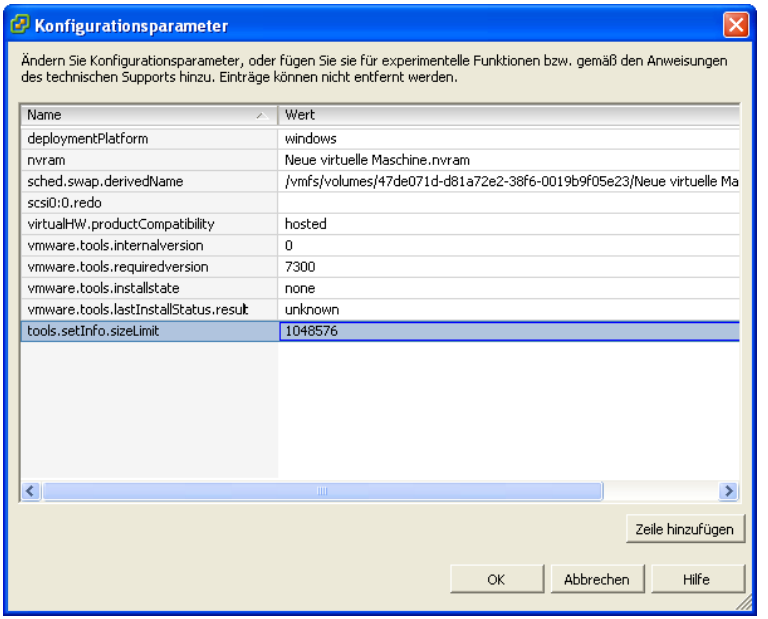
3 Klicken Sie auf **Optionen (Options)** > **Erweitert (Advanced)** > **Konfigurationsparameter (Configuration Parameters)**. Das Dialogfeld **Konfigurationsparameter (Configuration Parameters)** wird geöffnet.

4 Wenn das Attribut zur Größenbegrenzung nicht vorhanden ist, klicken Sie auf **Zeile hinzufügen (Add Row)**, und geben Sie Folgendes ein:

   - **Feld „Name“** – **`tools.setInfo.sizeLimit`**
   - **Feld „Wert“** – **`<Anzahl der Bytes>`**

   Wenn das Größenlimitattribut vorhanden ist, passen Sie es wie gewünscht an.

Eine Konfiguration mit der **GuestInfo**-Größe von 1 MB sieht so aus:



5 Klicken Sie auf **OK**, um das Dialogfeld **Konfigurationsparameter (Configuration Parameters)** zu schließen, und dann noch einmal auf **OK**, um das Dialogfeld **Eigenschaften der virtuellen Maschinen (Virtual Machine Properties)** zu schließen.

Sie können auch vollständig verhindern, dass Gäste Name/Wert-Paare in die Konfigurationsdatei schreiben. Dies bietet sich an, wenn Gastbetriebssysteme am Ändern von Konfigurationseinstellungen gehindert werden müssen.

So hindern Sie Gastbetriebssystemprozesse am Senden von Konfigurationsnachrichten an den Host

1 Melden Sie sich am VI-Client an, und wählen Sie die virtuelle Maschine in der Bestandsliste aus.

Die Konfiguration für diese virtuelle Maschine wird auf der Registerkarte **Übersicht (Summary)** angezeigt.

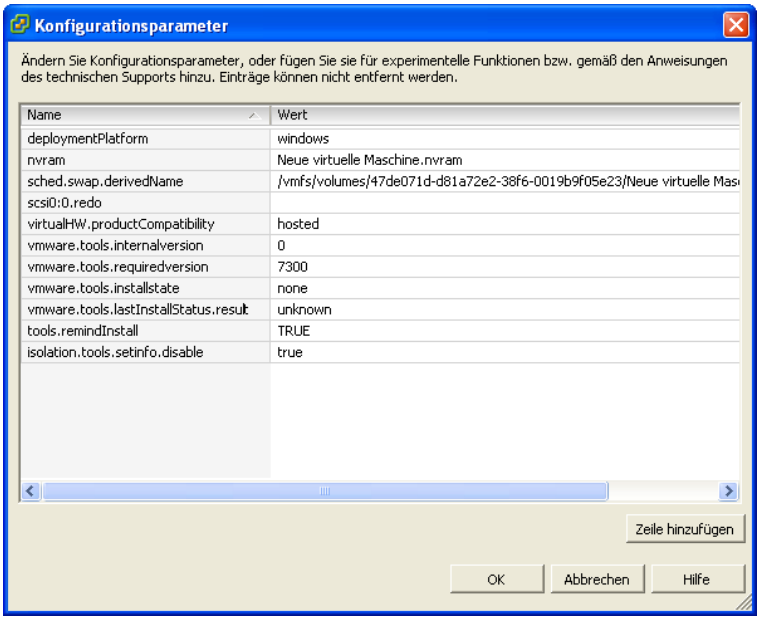
2 Klicken Sie auf **Einstellungen bearbeiten (Edit Settings)**.

3 Klicken Sie auf **Optionen (Options)** > **Erweitert (Advanced)** > **Konfigurationsparameter (Configuration Parameters)**. Das Dialogfeld **Konfigurationsparameter (Configuration Parameters)** wird geöffnet.

4 Klicken Sie auf die Schaltfläche **Hinzufügen (Add)** und geben Sie Folgendes ein:

- **Feld „Name“ – `isolation.tools.setinfo.disable`**
- **Feld „Wert“ – `true`**

Das Ergebnis sieht folgendermaßen aus.



5 Klicken Sie auf **OK**, um das Dialogfeld **Konfigurationsparameter (Configuration Parameters)** zu schließen, und dann noch einmal auf **OK**, um das Dialogfeld **Eigenschaften der virtuellen Maschinen (Virtual Machine Properties)** zu schließen.

Konfigurieren der Protokollierungsebenen für das Gastbetriebssystem

Virtuelle Maschinen können Informationen zur Fehlerbehebung in eine Protokolldatei der virtuellen Maschine schreiben, die auf dem VMFS-Volume gespeichert wird. Benutzer und Prozesse virtueller Maschinen können die Protokollierung entweder absichtlich oder unabsichtlich missbrauchen, sodass große Datenmengen die Protokolldatei überfluten. Mit der Zeit kann die Protokolldatei so genug Speicherplatz im Dateisystem der Servicekonsole belegen, um einen Ausfall zu verursachen.

Um dieses Problem zu verhindern, können Sie die Protokollierung für die Gastbetriebssysteme virtueller Maschinen deaktivieren. Mit diesen Einstellungen können die Gesamtgröße und die Anzahl der Protokolldateien begrenzt werden. Normalerweise wird bei jedem Neustart eines Hosts eine neue Protokolldatei erstellt, sodass die Datei relativ schnell wachsen kann. Sie können jedoch dafür sorgen, dass die Erstellung neuer Protokolldateien öfter erfolgt, indem Sie die maximale Größe der Protokolldateien begrenzen. Wenn Sie die Gesamtgröße der Protokolldaten beschränken möchten, empfiehlt VMware das Speichern von 10 Protokolldateien mit maximal je 100 KB. Diese Werte sind klein genug, sodass die Protokolldateien nicht übermäßig viel Speicherplatz auf dem Host belegen sollten. Dennoch werden ausreichend Daten erfasst, die zum Beheben der meisten ggf. auftretenden Probleme erforderlich sind.

Immer wenn ein Eintrag in das Protokoll geschrieben wird, erfolgt eine Überprüfung der Protokollgröße. Ist der Grenzwert überschritten, wird der nächste Eintrag in ein neues Protokoll geschrieben. Wenn die maximale Anzahl an Protokolldateien erreicht ist, wird eine neue erstellt und die älteste gelöscht. Es könnte ein, diese Grenzwerte umgehender, Denial-of-Service-Angriff versucht werden, indem ein riesiger Protokolleintrag geschrieben wird. Jeder Protokolleintrag ist jedoch auf 4KB begrenzt, sodass eine Protokolldatei niemals mehr als 4KB größer als der konfigurierte Grenzwert sein kann.

So begrenzen Sie die Anzahl und Größe von Protokolldateien

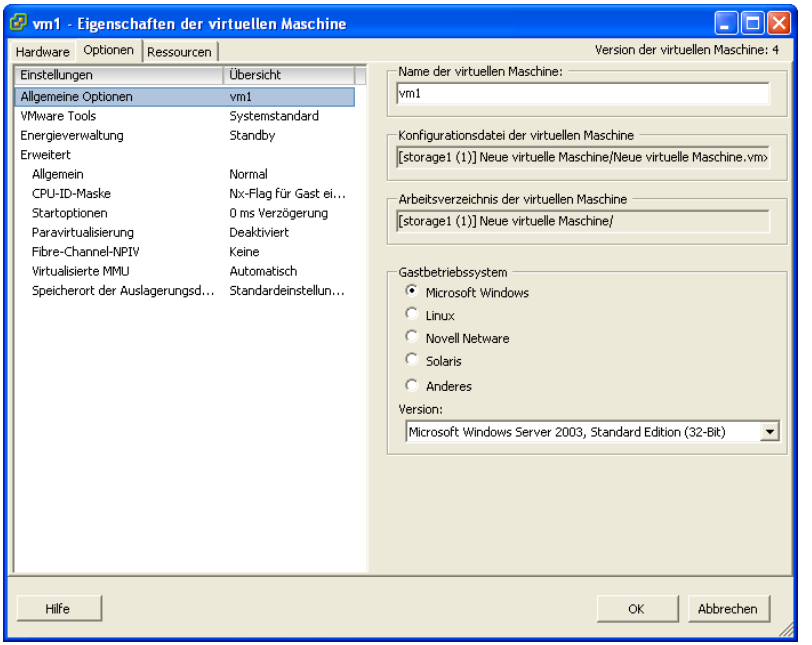
1 Melden Sie sich am VI-Client an, und wählen Sie die virtuelle Maschine in der Bestandsliste aus.

   Die Konfiguration für diese virtuelle Maschine wird auf der Registerkarte **Übersicht (Summary)** angezeigt.

2 Klicken Sie auf **Einstellungen bearbeiten (Edit Setting)**.

   Das Dialogfeld mit den Eigenschaften der virtuellen Maschine wird geöffnet.

3 Klicken Sie auf **Optionen (Options)** > **Allgemein (General)**, und notieren Sie sich den Pfad, der im Feld **Konfigurationsdatei der virtuellen Maschine (Virtual Machine Configuration File)** angezeigt wird.



4 Melden Sie sich an der Servicekonsole an, und rufen Sie Root-Berechtigungen ab. Wechseln Sie in das Verzeichnis, um auf die Konfigurationsdatei der virtuellen Maschine zuzugreifen, deren Pfad Sie sich in Schritt Schritt 3 notiert haben.

Die Konfigurationsdateien der virtuellen Maschinen befinden sich im Verzeichnis `/vmfs/volumes/<Datenspeicher>`, wobei es sich bei `<Datenspeicher>` um den Namen des Speichergeräts handelt, auf dem die Dateien der virtuellen Maschine gespeichert sind. Wenn beispielsweise die Konfigurationsdatei der virtuellen Maschine, die Sie im Dialogfeld **Eigenschaften der virtuellen Maschine (Virtual Machine Properties)** abgerufen haben, `[vol1]vm-finance/vm-finance.vmx` ist, wechseln Sie die Verzeichnisse wie folgt:

```
cd /vmfs/volumes/vol1/vm-finance/
```

5 Verwenden Sie zum Begrenzen der Protokollgröße Nano oder einen anderen Text-Editor, um die `.vmx`-Datei um die folgende Zeile zu ergänzen.

```
log.rotateSize=<Maximalgröße>
```

`<Maximalgröße>` ist die maximale Dateigröße in Bytes. Um beispielsweise die Datei auf 100 KB zu begrenzen, geben Sie **`100000`** ein.

6 Verwenden Sie zum Begrenzen der Anzahl der Protokolldateien Nano oder einen anderen Text-Editor, um die `.vmx`-Datei um die folgende Zeile zu ergänzen.

`log.keepOld=<Gewünschte Anzahl an Dateien>`

`<Gewünschte Anzahl an Dateien>` ist die Anzahl an Dateien, die auf dem Server gespeichert bleiben. Um beispielsweise 10 Protokolldateien zu speichern und anschließend mit dem Löschen der ältesten und Erstellen neuer Dateien zu beginnen, geben Sie **`10`** ein.

Die Protokollierung kann auch vollständig deaktiviert werden. Beachten Sie, dass Sie in diesem Fall ggf. nicht in der Lage sind, entsprechende Protokolle für die Fehlerbehebung zu sammeln. Außerdem leistet VMware keine technische Unterstützung für virtuelle Maschinen, bei denen die Protokollierung deaktiviert wurde.

So deaktivieren Sie die Protokollierung für das Gastbetriebssystem

1 Melden Sie sich am VI-Client an, und wählen Sie die virtuelle Maschine in der Bestandsliste aus.

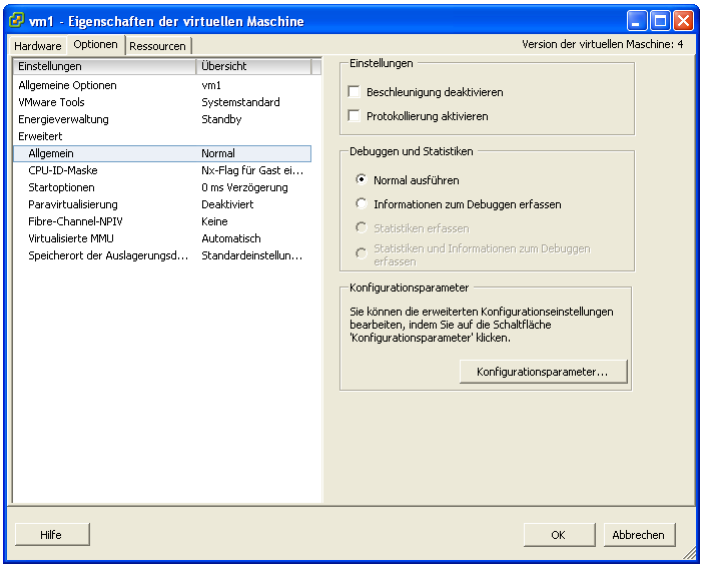
Die Konfiguration für diese virtuelle Maschine wird auf der Registerkarte **Übersicht (Summary)** angezeigt.

2 Klicken Sie auf **Einstellungen bearbeiten (Edit Settings)**.

3 Klicken Sie auf **Optionen (Options)** > **Erweitert (Advanced)** > **Allgemein (General)**.

4 Deaktivieren Sie das Kontrollkästchen **Protokollierung aktivieren (Enable logging)**.

Das Ergebnis sieht folgendermaßen aus.



5 Klicken Sie auf **OK**, um zum Dialogfeld **Eigenschaften der virtuellen Maschine (Virtual Machine Properties)** zurückzukehren.

Anhänge

Befehle für den technischen Support von ESX Server 3

A

In diesem Anhang werden die Servicekonsolenbefehle vorgestellt, mit denen der ESX Server 3 konfiguriert wird. Die meisten dieser Befehle sind nur für die Verwendung durch den technischen Support vorgesehen und hier nur zu rein informativen Zwecken aufgeführt. In einigen wenigen Fällen sind diese Befehle jedoch das einzige Mittel zur Ausführung einer bestimmten Konfigurationsaufgabe für den ESX Server 3-Host. Wenn etwa die Verbindung zum Host unterbrochen wird, kann die Ausführung gewisser Befehle über die Befehlszeilenoberfläche Ihr einziger Ausweg sein – beispielsweise, wenn das Netzwerk ausfällt und ein Zugriff über den VI-Client deshalb nicht möglich ist.

HINWEIS Wenn Sie die Befehle in diesem Anhang verwenden, müssen Sie den Befehl `service mgmt-vmware restart` ausführen, um den Prozess `vmware-hostd` neu zu starten und den VI-Client und andere Management-Programme auf die Änderungen der Konfiguration aufmerksam zu machen. Im Allgemeinen sollten Sie die Ausführung der Befehle in diesem Anhang vermeiden, wenn der Host gegenwärtig durch den VI-Client oder den VirtualCenter Server verwaltet wird.

Die grafische Benutzeroberfläche des VI-Clients ist die bevorzugte Umgebung zur Ausführung der Konfigurationsaufgaben, die in diesem Anhang beschrieben werden. Sie können diesen Anhang verwenden, wenn Sie wissen möchten, welche VI-Client-Befehle anstelle der Servicekonsolenbefehle verwendet werden können. Dieser Anhang bietet eine Übersicht der Aktionen, die Sie im VI-Client durchführen können, bietet jedoch keine vollständigen Anleitungen. Details zur Verwendung der Befehle und zur Ausführung von Konfigurationsaufgaben über den VI-Client finden Sie in der Onlinehilfe.

Zusätzliche Informationen zu bestimmten ESX Server 3-Befehlen erhalten Sie, wenn Sie sich an der Servicekonsole anmelden und über den Befehl `man <esxcfg_Befehlsname>` die entsprechenden Manpages anzeigen lassen.

Tabelle A-1 führt die Befehle für den technischen Support für ESX Server 3 auf, fasst den Zweck jedes Befehls zusammen und bietet eine Alternative zum VI-Client. Sie können die meisten der VI-Client-Aktionen, die in der Tabelle aufgeführt werden, erst dann ausführen, wenn Sie einen ESX Server 3-Host in der Bestandsliste ausgewählt und auf die Registerkarte **Konfiguration (Configuration)** geklickt haben. Dies muss vor der Ausführung der unten aufgeführten Prozeduren durchgeführt werden, sofern nichts anderes angegeben ist.

Tabelle A-1. Befehle für den technischen Support von ESX Server 3

Servicekonsolenbefehl	Zweck des Befehls und VI Client-Verfahren
`esxcfg-advcfg`	Konfiguriert erweiterte Optionen für ESX Server 3. Um die erweiterten Optionen im VI-Client zu konfigurieren, klicken Sie auf **Erweiterte Einstellungen (Advanced Settings)**. Wenn das Dialogfeld **Erweiterte Einstellungen (Advanced Settings)** geöffnet wird, wählen Sie in der Liste auf der linken Seite den Gerätetyp oder die Aktivität aus, mit dem/der Sie arbeiten möchten, und nehmen Sie die entsprechenden Einstellungen vor.
`esxcfg-auth`	Konfiguriert die Authentifizierung. Verwenden Sie diesen Befehl, um zwischen den Plug-Ins `pam_cracklib.so` und `pam_passwdqc.so` zur Durchsetzung der Änderungsregeln für Kennwörter umzuschalten. Mit diesem Befehl können Sie auch die Optionen für diese beiden Plug-Ins zurücksetzen. Weitere Informationen finden Sie unter „Kennwortkomplexität“ auf Seite 256 Diese Funktionen können nicht im VI-Client konfiguriert werden.
`esxcfg-boot`	Konfiguriert die Bootstrap-Einstellungen. Dieser Befehl wird für den Bootstrap-Prozess verwendet und ist nur für den technischen Support von VMware vorgesehen. Geben Sie diesen Befehl nur auf ausdrückliche Anweisung eines Vertreters des technischen Suports von VMware ein. Diese Funktionen können nicht im VI-Client konfiguriert werden.

Tabelle A-1. Befehle für den technischen Support von ESX Server 3 (Fortsetzung)

Servicekonsolenbefehl	Zweck des Befehls und VI Client-Verfahren
`esxcfg-dumppart`	Konfiguriert eine Diagnosepartition oder sucht nach bestehenden Diagnosepartitionen. Bei der Installation des ESX Server 3 wird eine Diagnosepartition zur Speicherung von Informationen zur Fehlersuche erstellt, wenn ein Systemfehler auftritt. Sie müssen diese Partition nicht manuell anlegen, es sei denn Sie stellen fest, dass es keine Diagnosepartition für den Host gibt. Für Diagnosepartitionen stehen im VI-Client folgende Verwaltungsvorgänge zur Verfügung: ■ **Vorhandensein einer Diagnosepartition bestimmen** — Klicken Sie auf **Speicher (Storage)** > **Hinzufügen (Add)**, und überprüfen Sie die erste Seite des Assistenten zum Hinzufügen von Speicher, ob dort die Option **Diagnose (Diagnostic)** aufgeführt wird. Wenn **Diagnose (Diagnostic)** nicht zu den Optionen zählt, verfügt ESX Server 3 bereits über eine Diagnosepartition. ■ **Eine Diagnosepartition konfigurieren** — Klicken Sie auf **Speicher (Storage)** > **Hinzufügen (Add)** > **Diagnose (Diagnostic)**, und folgen Sie den Anweisungen des Assistenten.
`esxcfg-firewall`	Konfiguriert die Ports der Servicekonsolen-Firewall. Wählen Sie zur Konfiguration der Firewallports für unterstützte Dienste und Assistenten im VI-Client die Internetdienste aus, die auf den ESX Server 3-Host zugreifen dürfen. Klicken Sie auf **Sicherheitsprofil (Security Profile)** > **Firewall** > **Eigenschaften (Properties)**, und fügen Sie über das Dialogfeld **Firewall-Eigenschaften (Firewall Properties)** Dienste hinzu. Weitere Informationen zum Hinzufügen von Diensten und zur Konfiguration von Firewalls finden Sie unter „Öffnen von Firewallports für unterstützte Dienste und Verwaltungs-Agenten“ auf Seite 198. Sie können im VI-Client keine nicht unterstützten Dienste konfigurieren. Verwenden Sie für diese Dienste den Befehl `esxcfg-firewall` (siehe„Konfiguration der Servicekonsolen-Firewall“ auf Seite 249).
`esxcfg-info`	Druckt Informationen zum Status der Servicekonsole, des VMkernels, verschiedener Untersysteme im virtuellen Netzwerk und zur Speicherressourcen-Hardware aus. Mit dem VI-Client können diese Informationen nicht ausgedruckt werden, jedoch können die meisten Informationen jedoch können über verschiedene Registerkarten und Funktionen in der Benutzeroberfläche ermittelt werden. So können Sie zum Beispiel den Status der virtuellen Maschinen auf der Registerkarte **Virtuelle Maschinen (Virtual Machines)** überprüfen.
`esxcfg-init`	Führt interne Initialisierungsroutinen aus. Dieser Befehl wird für den Bootstrap-Prozess verwendet und sollte unter keinen Umständen ausgeführt werden. Dieser Befehl kann zu Problemen mit dem ESX Server 3-Host führen. Es gibt keine VI-Client-Entsprechung für diesen Befehl.

Tabelle A-1. Befehle für den technischen Support von ESX Server 3 (Fortsetzung)

Servicekonsolenbefehl	Zweck des Befehls und VI Client-Verfahren
`esxcfg-linuxnet`	Konvertiert beim Start von ESX Server 3 `vswif` in `eth`, wodurch der Modus „Nur Servicekonsole“ anstelle des ESX-Modus gestartet wird. Dieser Befehl wird für den Bootstrap-Prozess verwendet und ist nur für den technischen Support von VMware vorgesehen. Geben Sie diesen Befehl nur auf ausdrückliche Anweisung eines Vertreters des technischen Supports von VMware ein. Es gibt keine VI-Client-Entsprechung für diesen Befehl.
`esxcfg-module`	Legt die Treiberparameter fest und ändert die Einstellung, welche Treiber während des Hochfahrens geladen werden. Dieser Befehl wird für den Bootstrap-Prozess verwendet und ist nur für den technischen Support von VMware vorgesehen. Geben Sie diesen Befehl nur auf ausdrückliche Anweisung eines Vertreters des technischen Supports von VMware ein. Es gibt keine VI-Client-Entsprechung für diesen Befehl.
`esxcfg-mpath`	Konfiguriert die Multipath-Einstellungen für Fibre-Channel- oder iSCSI-Festplatten. Klicken Sie zur Konfiguration der Multipath-Einstellungen für den Speicher im VI-Client auf **Speicher (Storage)**. Wählen Sie einen Datenspeicher oder eine zugeordnete LUN aus, und klicken Sie auf **Eigenschaften (Properties)**. Wählen Sie ggf. im Dialogfeld **Eigenschaften (Properties)** die gewünschte Erweiterung aus. Klicken Sie dann auf **Gerät erweitern (Extent Device)** > **Pfade verwalten**, und konfigurieren Sie die Pfade über das Dialogfeld **Pfad verwalten (Manage Paths)**.
`esxcfg-nas`	Verwaltet die NAS-Mounts. Mit diesem Befehl können Sie NAS-Geräte hinzufügen, löschen, auflisten oder ihre Attribute ändern. Klicken Sie zur Anzeige der NAS-Geräte im VI-Client auf **Speicher (Storage)**, und scrollen Sie durch die Speicherliste. In der Ansicht **Speicher (Storage)** können Sie außerdem folgende Vorgänge ausführen: ■ **Attribute eines NAS-Geräts anzeigen** — Klicken Sie auf das Gerät, und überprüfen Sie die Informationen unter **Details**. ■ **NAS-Gerät hinzufügen** — Klicken Sie auf **Speicher hinzufügen (Add Storage)**. ■ **NAS-Gerät löschen** — Klicken Sie auf **Entfernen (Remove)**. ■ **Attribute eines NAS-Geräts ändern** — Klicken Sie auf das Gerät und dann auf **Details** > **Eigenschaften (Properties)**. Eine vollständige Anleitung zur Erstellung und Konfiguration von NAS-Datenspeichern finden Sie unter „Konfigurieren von ESX Server 3 für den Zugriff auf NFS-Volumes“ auf Seite 137.

Tabelle A-1. Befehle für den technischen Support von ESX Server 3 (Fortsetzung)

Servicekonsolenbefehl	Zweck des Befehls und VI Client-Verfahren
`esxcfg-nics`	Druckt eine Liste der physischen Netzwerkadapter sowie Informationen zum Treiber, dem PCI-Gerät und dem Verbindungsstatus der einzelnen Netzwerkkarten. Sie können diesen Befehl auch verwenden, um die Geschwindigkeit und den Duplexmodus eines physischen Netzwerkadapters zu steuern. Die Informationen zu den physischen Netzwerkadaptern des Hosts können Sie im VI-Client anzeigen, indem Sie auf **Netzwerkadapter (Network Adapters)** klicken. Klicken Sie zur Änderung der Geschwindigkeit und des Duplexmodus für einen physischen Netzwerkadapter im VI-Client bei einem virtuellen Switch, der dem physischen Netzwerkadapter zugeordnet wurde, auf **Netzwerk (Networking)** > **Eigenschaften (Properties)**. Klicken Sie dann im Dialogfeld **Eigenschaften (Properties)** auf **Netzwerkadapter (Network Adapters)** > **Bearbeiten (Edit)**, und wählen Sie die Geschwindigkeit/Duplex-Kombination aus. Weitere Informationen zur Änderung der Geschwindigkeit und des Duplexmodus finden Sie unter „So konfigurieren Sie die Geschwindigkeit des Uplink-Netzwerkadapters“ auf Seite 44.
`esxcfg-resgrp`	Stellt die Ressourcengruppeneinstellungen wieder her und ermöglicht die Ausführung grundlegender Verwaltungsaufgaben für Ressourcengruppen. Wählen Sie einen Ressourcenpool im Bestandslistenfenster aus, und klicken Sie auf der Registerkarte **Übersicht (Summary)** auf **Einstellungen bearbeiten (Edit Settings)**, um die Einstellungen der Ressourcengruppe zu ändern.
`esxcfg-route`	Dient zum Festlegen bzw. Abrufen der standardmäßigen VMkernel-Gatewayroute sowie zum Hinzufügen, Entfernen und Auflisten statischer Routen. Um die Standard-Gatewayroute des VMkernels im VI-Client festzulegen, klicken Sie auf **DNS und Routing (DNS and Routing)**. Wenn Sie die Standardroute ändern möchten, klicken Sie auf **Eigenschaften (Properties)**, und aktualisieren Sie die Daten auf beiden Registerkarten im Dialogfeld **DNS- und Routing-Konfiguration (DNS and Routing Configuration)**.
`esxcfg-swiscsi`	Konfiguriert den Software-iSCSI-Software-Adapter. Klicken Sie zur Konfiguration des Software-iSCSI-Systems im VI-Client auf **Speicheradapter (Storage Adapters)**, markieren Sie den iSCSI-Adapter, den Sie konfigurieren möchten, und klicken Sie auf **Eigenschaften (Properties)**. Konfigurieren Sie den Adapter im Dialogfeld **Eigenschaften des iSCSI-Initiators (iSCSI Initiator Properties)**. Eine vollständige Anleitung zur Erstellung und Konfiguration von iSCSI-Datenspeichern finden Sie unter „iSCSI-Speicher“ auf Seite 116.

Tabelle A-1. Befehle für den technischen Support von ESX Server 3 (Fortsetzung)

Servicekonsolenbefehl	Zweck des Befehls und VI Client-Verfahren
`esxcfg-upgrade`	Aktualisiert ESX Server von ESX Server 2.*x* auf ESX Server 3. Dieser Befehl ist nicht zur allgemeinen Verwendung bestimmt. Durch das Upgrade von 2.x auf 3.x werden die folgenden Aufgaben ausgeführt. Einige davon können im VI-Client ausgeführt werden: ■ **Aktualisierung des Hosts** — Beim Upgrade von ESX Server 2.*x* auf ESX Server 3 werden die Binärdateien aktualisiert. Diesen Schritt können Sie nicht über den VI-Client ausführen. Informationen zur Durchführung dieser Aktualisierung erhalten Sie im *Installations- und Upgrade-Handbuch*. ■ **Aktualisierung des Dateisystems** — Wenn Sie VMFS-2 auf VMFS-3 aktualisieren möchten, halten Sie Ihre virtuellen Maschinen an oder fahren Sie sie herunter und klicken Sie dann auf **Bestandsliste (Inventory)** > **Host** > **In den Wartungsmodus wechseln (Enter Maintenance Mode)**. Klicken Sie auf **Speicher (Storage)**, wählen Sie ein Speichergerät aus, und klicken Sie auf **Auf VMFS-3 aktualisieren (Upgrade to VMFS-3)**. Sie müssen diesen Schritt für jedes Speichergerät ausführen, das Sie aktualisieren möchten. ■ **Upgrade der virtuellen Maschinen** — Um eine virtuelle Maschine von VMS-2 auf VMS-3 zu aktualisieren, klicken Sie mit der rechten Maustaste auf die virtuelle Maschine im Bestandslistenfenster, und wählen Sie **Virtuelle Maschine aktualisieren (Upgrade Virtual Machine)**.
`esxcfg-vmhbadevs`	Druckt eine Zuordnung von VMkernel-Speichergeräten zu Servicekonsolengeräten. Es gibt keine VI-Client-Entsprechung für diesen Befehl.
`esxcfg-vmknic`	Erstellt und aktualisiert VMkernel-TCP/IP-Einstellungen für VMotion, NAS und iSCSI. Um VMotion-, NFS- oder iSCSI-Netzwerkverbindungen einzurichten, klicken Sie im VI Client auf **Netzwerk (Networking) > Netzwerk hinzufügen (Add Networking)**. Wählen Sie **VMkernel** aus, und folgen Sie den Anweisungen des Assistent zum Hinzufügen von Netzwerken. Definieren Sie die IP-Adresse-Subnetzmask und den VMkernel-Standardgateway im Schritt **Verbindungseinstellungen (Connection Settings)**. Wenn Sie die Einstellungen überprüfen möchten, klicken Sie auf das blaue Symbol links neben dem VMotion-, iSCSI- oder NFS-Port. Wenn Sie eine der Einstellungen bearbeiten möchten, klicken Sie für den entsprechenden Switch auf **Eigenschaften (Properties)**. Wählen Sie den Port in der Liste im Dialogfeld **Eigenschaften (Properties)** aus, und klicken Sie auf **Bearbeiten (Edit)**, um das Dialogfeld **Eigenschaften (Properties)** des Ports zu öffnen und die Einstellungen des Ports zu ändern. Eine vollständige Anleitung zur Erstellung und Aktualisierung von Netzwerkverbindungen für VMotion, NFS oder iSCSI finden Sie unter „Netzwerkkonfiguration des VMkernels“ auf Seite 30.

Tabelle A-1. Befehle für den technischen Support von ESX Server 3 (Fortsetzung)

Servicekonsolenbefehl	Zweck des Befehls und VI Client-Verfahren
`esxcfg-vswif`	Erstellt und aktualisiert die Netzwerkeinstellungen der Servicekonsole. Dieser Befehl wird verwendet, wenn Sie den ESX Server 3-Host aufgrund von Problemen mit der Netzwerkkonfiguration nicht über den VI-Client verwalten können. Weitere Informationen finden Sie unter „Fehlerbehebung bei der Vernetzung der Servicekonsole“ auf Seite 85 Um VMotion-, NFS- oder iSCSI-Netzwerkverbindungen im VI-Client einzurichten, klicken Sie auf **Netzwerk (Networking) > Netzwerk hinzufügen (Add Networking)**. Wählen Sie **Servicekonsole (Service Console)** aus, und folgen Sie den Anweisungen des Assistenten zum Hinzufügen von Netzwerken. Im Schritt **Verbindungseinstellungen (Connection Settings)** werden die Subnetzmaske der IP-Adresse und der Standard-Gateway der Servicekonsole eingerichtet. Wenn Sie die Einstellungen überprüfen möchten, klicken Sie auf das blaue Symbol links neben dem Servicekonsolenport. Wenn Sie eine der Einstellungen bearbeiten möchten, klicken Sie für den entsprechenden Switch auf **Eigenschaften (Properties)**. Wählen Sie den Servicekonsolenport in der Liste im Dialogfeld **Eigenschaften (Properties)** des Switches aus. Klicken Sie auf **Bearbeiten (Edit)**, um das Dialogfeld **Eigenschaften (Properties)** des Ports zu öffnen und dessen Einstellungen zu ändern. Eine vollständige Anleitung zur Erstellung und Aktualisierung der Servicekonsolenverbindung finden Sie unter „Konfiguration der Servicekonsole“ auf Seite 34.
`esxcfg-vswitch`	Erstellt und aktualisiert die Netzwerkeinstellungen für virtuelle Maschinen. Klicken Sie zur Einrichtung von Verbindungen für eine virtuelle Maschine im VI-Client auf **Netzwerk (Networking) > Netzwerk hinzufügen (Add Networking)**. Wählen Sie **Virtuelle Maschine (Virtual Machine)** aus, und folgen Sie den Anweisungen des Assistenten zum Hinzufügen von Netzwerken (Add Network Wizard). Wenn Sie die Einstellungen überprüfen möchten, klicken Sie auf das Sprechblasen-Symbol links neben der gewünschten Portgruppe der virtuellen Maschine. Wenn Sie eine der Einstellungen bearbeiten möchten, klicken Sie für den entsprechenden Switch auf **Eigenschaften (Properties)**. Wählen Sie den Port der virtuellen Maschine in der Liste im Dialogfeld **Eigenschaften (Properties)** des Switches aus, und klicken Sie auf **Bearbeiten (Edit)**, um das Dialogfeld **Eigenschaften (Properties)** des Ports zu öffnen und dessen Einstellungen zu ändern. Eine vollständige Anleitung zur Erstellung und Aktualisierung von virtuellen Maschinen finden Sie unter „Konfiguration virtueller Netzwerke für virtuelle Maschinen“ auf Seite 27.

Andere Befehle

Um bestimmte interne Vorgänge zu unterstützen, enthalten die ESX Server 3-Installationen eine Reihe standardmäßiger Linux-Konfigurationsbefehle, wie beispielsweise Befehle zur Konfiguration von Netzwerken und Speichern. Eine Verwendung dieser Befehle zur Ausführung von Konfigurationsaufgaben kann einerseits zu schwerwiegenden Konfigurationskonflikten führen und andererseits auch dazu, dass bestimmte ESX Server 3-Funktionen nicht mehr verwendet werden können. Arbeiten Sie immer mit dem VI-Client, um ESX Server 3 zu konfigurieren, es sei denn, die VMware Infrastructure-Dokumentation oder der technische Support von VMware geben Ihnen andere Anweisungen.

Verwenden von „vmkfstools“

B

Sie verwenden das Dienstprogramm `vmkfstools`, um virtuelle Festplatten, Dateisysteme, logische Volumes und physische Speichergeräte auf dem VMware ESX Server-Host anzulegen und einzurichten. Mithilfe von `vmkfstools` können Sie das VMFS (Virtual Machine File System, Dateisystem der virtuellen Maschine) auf einer physischen Partition einer Festplatte anlegen und verwalten. Sie können dieses Programm auch dazu verwenden, Dateien wie virtuelle Festplatten zu bearbeiten, die auf VMFS-2, VMFS-3 und NFS gespeichert sind.

Sie können die meisten `vmkfstools`-Aufgaben auch über den VI-Client ausführen. Weitere Informationen zur Verwendung des VI-Clients zur Speicherverwaltung finden Sie unter „Speicherkonfiguration“ auf Seite 109.

Dieser Anhang behandelt die folgenden Abschnitte:

- „vmkfstools-Befehlssyntax“ auf Seite 300
- „vmkfstools-Optionen“ auf Seite 301

vmkfstools-Befehlssyntax

Im Allgemeinen müssen Sie sich nicht als Root-Benutzer anmelden, um die `vmkfstools`-Befehle auszuführen. Einige Befehle, z. B. Dateisystembefehle, erfordern jedoch eine Root-Anmeldung.

Verwenden Sie mit dem `vmkfstools`-Befehl die folgenden Argumente:

- Bei `<options>` handelt es sich um eine oder mehrere Befehlszeilenoptionen und die zugehörigen Argumente, mit denen Sie die Aktivität angeben können, die `vmkfstools` ausführen soll. Hierzu gehört beispielsweise die Auswahl des Festplattenformats beim Erstellen einer neuen virtuellen Festplatte.

  Nach der Eingabe dieser Option, geben Sie eine Datei oder ein VMFS-Dateisystem an, auf dem Sie den Vorgang ausführen möchten, indem Sie einen relativen oder absoluten Dateipfadnamen in der Hierarchie `/vmfs` eingeben.

- `<Partition>` bezeichnet die Festplattenpartitionen. Dieses Argument verwendet ein `vmhbaA:T:L:P`-Format, bei dem es sich bei `A`, `T`, `L` und `P` um Ganzzahlen handelt, die den Adapter, das Ziel, die LUN und die Partitionsnummer bezeichnen. Diese Zahl der Partition muss größer als Null sein und der gültigen VMFS-Partition des Typs `fb` entsprechen.

  `vmhba0:2:3:1` beispielsweise bezieht sich auf die erste Partition auf LUN 3, Ziel 2, HBA 0.

- `<device>` bezeichnet Geräte oder logische Volumes. Dieses Argument verwendet einen Pfadnamen im ESX Server 3-Gerätedateisystem. Der Pfadname beginnt mit `/vmfs/devices`, wobei es sich um den Mount-Punkt des Gerätedateisystems handelt.

  Verwenden Sie zur Angabe der verschiedenen Gerätetypen die folgenden Formate:

  - `/vmfs/devices/disks` für lokale oder SAN-basierte Festplatten.
  - `/vmfs/devices/lvm` für logische ESX Server 3-Volumes.
  - `/vmfs/devices/generic` für generische SCSI-Geräte, z. B.Bandlaufwerke.

- `<path>` bezeichnet ein VMFS-Dateisystem oder eine Datei. Bei diesem Argument handelt es sich um einen absoluten oder relativen Pfad, der einen symbolischen Link zu einem Verzeichnis, einer Raw-Gerätezuordnung oder einer Datei unter `/vmfs` aufführt.

  - Um ein VMFS-Dateisystem anzugeben, verwenden Sie dieses Format:

    `/vmfs/volumes/<Dateisystem–UUID>`

    oder

    `/vmfs/volumes/<Dateisystembezeichnung>`

- Um eine VMFS-Datei anzugeben, verwenden Sie dieses Format:

  ```
  /vmfs/volumes/<Dateisystembezeichnung|Dateisystem-UUID>/[dir]/
                myDisk.vmdk
  ```

  Sie brauchen nicht den gesamten Pfad anzugeben, wenn das aktuelle Arbeitsverzeichnis gleichzeitig das übergeordnete Verzeichnis von `myDisk.vmdk` ist.

Beispiel:

```
/vmfs/volumes/datastore1/rh9.vmdk
```

vmkfstools-Optionen

Dieser Abschnitt enthält eine Liste aller Optionen, die mit dem Befehl `vmkfstools` verwendet werden können. Einige der Aufgaben in diesem Abschnitt enthalten Optionen, die nur für Benutzer mit fortgeschrittenen Kenntnissen bestimmt sind.

Die Lang- und -Kurzformen (mit einem Buchstaben) der Optionen sind gleichwertig. So sind zum Beispiel die folgenden Befehle identisch:

```
vmkfstools ––createfs vmfs3 ––blocksize 2m vmhba1:3:0:1
vmkfstools –C vmfs3 –b 2m vmhba1:3:0:1
```

Unteroption -v

Die Unteroption –v bestimmt die Ausführlichkeit der Meldungen in der Befehlsausgabe. Das Format für diese Unteroption lautet wie folgt:

```
–v ––verbose <Zahl>
```

Der Wert <Zahl> wird als ganze Zahl von 1 bis 10 angegeben.

Sie können die Unteroption –v für alle `vmkfstools`-Optionen verwenden. Wenn die Unteroption –v für die Ausgabe einer Option nicht vorgesehen ist, ignoriert `vmkfstools` den Teil –v der Befehlszeile.

HINWEIS Da Sie die Unteroption –v in jeder `vmkfstools`-Befehlszeile verwenden können, wird sie nicht in den Beschreibungen der einzelnen Optionen verwendet.

Dateisystemoptionen

Mithilfe von Dateisystemoptionen können Sie ein VMFS-Dateisystem erstellen. Diese Optionen gelten nicht für NFS. Sie können viele dieser Aufgaben auch über den VI-Client ausführen.

Erstellen eine VMFS-Dateisystems

```
-C --createfs vmfs3
        -b --blocksize <Blockgröße>kK|mM
        -S --setfsname <fsName>
```

Mit dieser Option wird ein VMFS-3-Dateisystem auf der angegebenen SCSI-Partition erstellt, z. B. `vmhba1:0:0:1`. Diese Partition wird die vorgelagerte Partition des Dateisystems.

VMFS-2-Dateisysteme sind auf ESX Server 3-Hosts schreibgeschützt. Benutzer können VMFS-2-Dateisysteme nicht erstellen oder ändern, aber die darauf gespeicherten Dateien lesen. Ein Zugriff über ESX 2.x-Hosts auf die VMFS-3-Dateisysteme ist nicht möglich.

VORSICHT Pro LUN ist nur ein VMFS-Volume möglich.

Für die Option `-C` können Sie folgende Unteroptionen angeben:

- `-b --blocksize` – Definiert die Blockgröße für das VMFS-3-Dateisystem. Die Standardblockgröße ist 1 MB. Der angebene Wert für `<block_size>` muss ein Vielfaches von 128 KB beim Mindestwert 128 KB sein. Wenn Sie die Größe angeben, müssen Sie auch die Einheit als Suffix „m“ bzw. „M“ angeben. Die Größeneinheit kann klein oder groß geschrieben werden. `vmkfstools` interpretiert „m“ bzw. „M“ als Megabytes und „k“ bzw. „K“ als Kilobyte.
- `-S --setfsname` – Definiert die Volume-Bezeichnung eines VMFS-Volumes für das VMFS-3-Dateisystem, das Sie erstellen. Für die Option `-C` können Sie folgende Unteroptionen angeben. Die Bezeichnung kann bis zu 128 Zeichen lang sein und darf keine Leerstellen am Anfang oder Ende enthalten.

  Nachdem Sie die Volume-Bezeichnung festgelegt haben, können Sie sie bei der Angabe des VMFS-Volumes im Befehl `vmkfstools` verwenden. Die Volume-Bezeichnung erscheint auch in den Auflistungen, die mit dem Linux-Befehl `ls -l` generiert werden, und als symbolische Verknüpfung zum VMFS-Volume im Verzeichnis `/vmfs/volumes`.

  Verwenden Sie den Linux-Befehl `ln -sf`, wenn Sie die VMFS-Volume-Bezeichnung ändern möchten. Beispiel:

  ```
  ln -sf /vmfs/volumes/<UUID> /vmfs/volumes/<fsName>
  ```

  `<fsName>` ist die neue Volume-Bezeichnung, die Sie für die `<UUID>` des VMFS verwenden möchten.

Erstellen eine VMFS-Dateisystems - Beispiel

```
vmkfstools –C vmfs3 –b 1m –S my_vmfs /vmfs/devices/disks/vmhba1:3:0:1
```

Dieses Beispiel veranschaulicht die Erstellung eines neuen VMFS-3-Dateisystems mit dem Namen `myvmfs` auf der ersten Partition von Ziel 3, LUN 0 des vmhba-Adapters 1. Die Dateiblockgröße beträgt 1 MB.

Erweitern eines bestehenden VMFS-3-Volumens

```
–Z ––extendfs <Erweiterungsgerät> <bestehendes_VMFS–Volume>
```

Diese Option fügt einem vorher erstellten VMFS-Volume, <`bestehendes VMFS–Volume`>, eine Erweiterung hinzu. Sie müssen den vollständigen Pfadnamen (Beispiel: `/vmfs/devices/disks/vmhba0:1:2:1`) und nicht nur den Kurznamen `vmhba0:1:2:1` angeben. Bei jeder Verwendung dieser Option wird das VMFS-3-Volume um eine neue Erweiterung vergrößert, sodass das Volume mehrere Partitionen umfasst. Ein logisches VMFS-3-Volume kann bis zu 32 physische Erweiterung aufweisen.

VORSICHT Wenn Sie diese Option ausführen, gehen alle Daten verloren, die auf dem SCSI-Gerät, das unter <`Erweiterungsgerät`> angegeben wird, gespeichert sind.

Beispiel für die Erweiterung eines VMFS-3 Volumes

```
vmkfstools –Z /vmfs/devices/disks/vmhba0:1:2:1
           /vmfs/devices/disks/vmhba1:3:0:1
```

Dieses Beispiel erweitert das logische Dateisystem durch Hinzufügen einer neuen Partition. Das erweiterte Dateisystem nimmt nun zwei Partitionen ein, `vmhba1:3:0:1` und `vmhba0:1:2:1`. In diesem Beispiel ist `vmhba1:3:0:1` der Name der übergeordneten Partition.

Auflisten der Attribute eines VMFS- Volumes

```
–P ––queryfs
        –h ––human–readable
```

Diese Option listet die Attribute des angegebenen Volumes auf, wenn Sie sie auf eine Datei oder ein Verzeichnis auf einem VMFS-Volume anwenden. Zu den aufgelisteten Attributen gehören die VMFS-Version (VMFS-2 oder VMFS-3), die Anzahl der Erweiterungen aus denen das angegebene VMFS-Volume besteht, die Volume-Bezeichnung (falls vorhanden), die UUID und eine Liste der Gerätenamen, auf denen sich die Erweiterungen befinden.

HINWEIS Wenn ein Gerät zur Sicherung des VMFS-Dateisystems offline geschaltet wird, ändert sich die Anzahl der Erweiterungen und des verfügbaren Speichers entsprechend.

Sie können die Unteroption `–h` für die Option `–P` verwenden. In diesem Fall listet `vmkfstools` die Kapazität des Volumes in verständlicherer Form auf, z. B. `5k`, `12.1M` oder `2.1G`.

Aktualisieren von VMFS-2 auf VMFS-3

Sie können ein VMFS-2-Dateisystem auf VMFS-3 aktualisieren.

VORSICHT Der Konvertierungsvorgang von VMFS-2 in VMFS-3 ist nicht umkehrbar. Nachdem das VMFS-2-Volume in VMFS-3 konvertiert wurde, kann es nicht in das Format VMFS-2 zurückkonvertiert werden.

Sie können ein VMFS-2-Dateisystem nur dann aktualisieren, wenn dessen Dateiblockgröße 8 MB nicht überschreitet.

Verwenden Sie folgende Optionen für die Aktualisierung des Dateisystems:

- `–T ––tovmfs3 –x ––upgradetype [zeroedthick|eagerzeroedthick|thin]`

  Diese Option konvertiert das VMFS-2-Dateisystem in VMFS-3 und erhält alle Dateien im Dateisystem. Entladen Sie vor der Konvertierung die `vmfs2`- und `vmfs3`-Treiber, und laden Sie den zusätzlichen Dateisystemtreiber `fsaux` mit der Moduloption `fsauxFunction=upgrade`.

  Sie müssen zum Angeben des Upgrade-Typs die Unteroption `–x ––upgradetype` auf eine der folgenden Varianten festlegen:

  - `–x zeroedthick` (default) – Behält die Eigenschaften der großen VMFS-2-Dateien bei. Mit dem Dateiformat `zeroedthick` wird den Dateien zur künftigen Nutzung ein Speicherplatz zugewiesen und die nicht verwendeten Datenblöcke werden nicht entfernt.
  - `–x eagerzeroedthick` – Entfernt während der Konvertierung ungenutzte Datenblöcke in großen Dateien. Wenn Sie diese Unteroption verwenden, dauert das Upgrade unter Umständen wesentlich länger als bei den anderen Optionen.
  - `–x thin` – Konvertiert große VMFS-2-Dateien in kleinere, bereitgestellte VMFS-3-Dateien. Im Gegensatz zum Format `thick` ermöglicht das Thin-Format es den Dateien nicht, für künftige Nutzungen einen zusätzlichen Speicherplatz zu verwenden, sondern stellt den Speicher nach Bedarf zur Verfügung. Während der Konvertierung werden unverwendete Blöcke der `thick` Dateien gelöscht.

Während der Konvertierung stellt der Dateisperrmechanismus von ESX Server 3 sicher, dass keine lokalen Prozesse auf das VMFS-Volume zugreifen, das konvertiert wird. Sie müssen gleichzeitig sicherstellen, dass kein ESX Server-Remotehost auf dieses Volume zugreift. Die Konvertierung kann mehrere Minuten dauern. Die Fertigstellung wird durch die Rückkehr zur Befehlszeileneingabe signalisiert.

Nach der Konvertierung deinstallieren Sie den `fsaux`-Treiber, und installieren Sie die `vmfs3`- und `vmfs2`-Treiber, um den normalen Betrieb wiederaufzunehmen.

- `-u --upgradefinish`

  Diese Option beendet das Upgrade.

Optionen für virtuelle Festplatten

Mithilfe von Optionen für virtuelle Festplatten können Sie in VMFS-2-, VMFS-3- und NFS-Dateisystemen gespeicherte virtuelle Festplatten einrichten, migrieren und verwalten. Sie können die meisten dieser Aufgaben auch über den VI-Client ausführen.

Unterstützte Festplattenformate

Beim Erstellen oder Klonen einer virtuellen Festplatte können Sie mit der Unteroption `-d --diskformat` das Format der Festplatte angeben. Wählen Sie eines der folgenden Formate aus:

- `zeroedthick` (Standardeinstellung) – Der Speicher, den die virtuelle Festplatte benötigt, wird während des Anlegens zugewiesen. Alle Daten, die auf dem physischen Gerät verbleiben, werden nicht während des Anlegens, sondern zu einem späteren Zeitpunkt während der ersten Schreibvorgänge der virtuellen Maschine gelöscht. Die virtuelle Maschine liest keine veralteten Daten von der Festplatte.
- `eagerzeroedthick` – Der Speicher, den die virtuelle Festplatte benötigt, wird während des Anlegens zugewiesen. Im Gegensatz zum `zeroedthick`-Format werden die verbleibenden Daten auf dem physischen Gerät während des Anlegens gelöscht. Das Anlegen von Festplatten in diesem Format kann wesentlich länger dauern als das Anlegen anderer Festplattentypen.
- `thick` – Der Speicher, den die virtuelle Festplatte benötigt, wird während des Anlegens zugewiesen. Bei dieser Art der Formatierung werden die alte Daten gelöscht, die sich ggf. im zugewiesenen Speicher befinden. Dieses Format darf nur vom Root-Benutzer erstellt werden.
- `thin` – „Schlank“ bereitgestellte virtuelle Festplatte. Im Gegensatz zum `Thick`-Format wird der erforderliche Speicher für die virtuelle Festplatte nicht während des Anlegens bereitgestellt, sondern später in gelöschter Form und nach Bedarf.

- `rdm` – Virtueller Kompatibilitätsmodus für die Raw-Gerätezuordnung.
- `rdmp` – Physischer Kompatibilitätsmodus (Pass-Through) für die Raw-Gerätezuordnung.
- `raw` – Raw-Gerät.
- `2gbsparse` – Eine Ersatzfestplatte mit höchstens 2 GB Erweiterungsgröße. Festplatten in diesem Format können mit anderen VMware Produkten verwendet werden. Sie können jedoch Ersatzfestplatten auf einem ESX Server-Host erst einschalten, nachdem Sie die Festplatte mithilfe von `vmkfstools` in einem kompatiblen Format (`thick` oder `thin`) erneut importiert haben.
- `monoflat` – Eine monolithische Ersatzfestplatte im Flat-Format. Festplatten in diesem Format können mit anderen VMware Produkten verwendet werden.
- monoflat – Eine monolithische Flat Disk. Festplatten in diesem Format können mit anderen VMware-Produkten verwendet werden.

HINWEIS Die einzigen Festplattenformate, die für NFS verwendet werden können, sind `thin`, `thick`, `zerodthick` und `2gbsparse`.

`Thick`, `zeroedthick` und `thin` bedeuten zumeist dasselbe, da der NFS-Server und nicht der ESX Server-Host die Zuordnungsrichtlinie festlegt. Die Standardzuordnungsrichtlinie auf den meisten NFS-Servern ist `thin`.

Erstellen eines virtuellen Laufwerks

```
-c --createvirtualdisk <Größe>[kK|mM|gG]
        -a --adaptertype [buslogic|lsilogic] <srcfile>
        -d --diskformat [thin|zeroedthick|eagerzeroedthick]
```

Diese Option erstellt eine virtuelle Festplatte im angegebenen Pfad auf einem VMFS-Volume. Legen Sie die Größe der virtuellen Festplatte fest. Wenn Sie für `<Größe>` einen Wert angeben, können Sie die Einheit festlegen, indem Sie entweder das Suffix `k` (Kilobyte) `m` (Megabyte) oder `g` (Gigabyte) angeben. Die Größeneinheit kann klein- oder großgeschrieben werden. `vmkfstools` interpretiert sowohl `k` als auch `K` als Kilobyte. Wenn Sie keine Einheit eingeben, ist die Standardeinstellung für `vmkfstools` Byte.

Für die Option `-c` können Sie folgende Unteroptionen angeben.

- `-a` gibt den Gerätetreiber an, der für die Kommunikation mit den virtuellen Festplatten verwendet wird. Sie haben die Auswahl zwischen den SCSI-Treibern von BusLogic und LSI Logic.
- `-d` bezeichnet die Festplattenformate. Eine detaillierte Beschreibung der Festplattenformate finden Sie unter „Unterstützte Festplattenformate“ auf Seite 305.

Beispiel der Erstellung einer virtuellen Festplatte

```
vmkfstools –c 2048m /vmfs/volumes/myVMFS/rh6.2.vmdk
```

Dieses Beispiel zeigt die Erstellung einer virtuellen Festplattendatei mit 2 GB und dem Namen `rh6.2.vmdk` im VMFS-Dateisystem mit dem Namen `myVMFS`. Diese Datei stellt eine leere virtuelle Festplatte dar, auf die virtuelle Maschinen zugreifen können.

Initialisieren einer virtuellen Festplatte

```
–w ––writezeros
```

Mit dieser Option wird die virtuelle Festplatte bereinigt, indem die gesamten Daten mit Nullen überschrieben werden. In Abhängigkeit der Größe Ihrer virtuellen Festplatte und der E/A-Bandbreite des Geräts, das als Host der virtuellen Festplatte dient, kann die Ausführung dieses Befehls lange dauern.

VORSICHT Bei der Ausführung dieses Befehls werden alle vorhandenen Daten auf der virtuellen Festplatte gelöscht.

Vergrößern einer virtuellen Festplatte im Thin-Format

```
–j ––inflatedisk
```

Mit dieser Option wird eine virtuelle Festplatte vom Typ `thin` in den Typ `eagerzeroedthick` konvertiert, wobei alle bestehenden Daten erhalten bleiben. Alle Blöcke, die nicht bereits nicht zugewiesen wurden, werden zugewiesen und gelöscht.

Siehe „Unterstützte Festplattenformate“ auf Seite 305.

Löschen einer virtuellen Festplatte

```
–U ––deletevirtualdisk
```

Diese Option löscht Dateien unter dem angegebenen Pfad auf dem VMFS-Volume, die einer virtuellen Festplatte zugeordnet sind.

Umbenennen eines virtuellen Laufwerks

```
–E ––renamevirtualdisk <alter Name> <neuer Name>
```

Diese Option benennt eine Datei einer virtuellen Festplatte um, die in der Pfadangabe der Befehlszeile angegeben wird. Sie können den ursprünglichen Dateinamen oder -pfad für `<alter Name>` und den neuen Dateinamen oder-pfad für `<neuer Name>` angeben.

Klonen einer virtuellen oder Raw-Festplatte

```
-i --importfile <Quelldatei> -d --diskformat
    [rdm:<Gerät>|rdmp:<Gerät>|
        raw:<Gerät>|thin|2gbsparse|monosparse|monoflat]
```

Diese Option erstellt eine Kopie einer virtuellen oder Raw-Festplatte, die Sie angeben.

Sie können die Unteroption `-d` für die Option `-i` verwenden. Diese Unteroption bezeichnet das Festplattenformat für die Kopie, die Sie anlegen. Siehe „Unterstützte Festplattenformate“ auf Seite 305. Nur Root-Benutzer dürfen eine virtuelle oder Raw-Festplatte klonen.

HINWEIS Um die ESX Server 3-Redo-Protokolle unter Beibehaltung ihrer Hierarchie zu klonen, verwenden Sie den Befehl `cp`.

Beispiel für das Klonen einer virtuellen Festplatte

```
vmkfstools -i /vmfs/volumes/templates/gold-master.vmdk
              /vmfs/volumes/myVMFS/myOS.vmdk
```

Dieses Beispiel veranschaulicht das Klonen der Inhalte einer virtuellen Master-Festplatte aus der Ablage `templates` , in eine virtuelle Festplattendatei mit der Bezeichnung `myOS.vmdk` auf dem Dateisystem mit der Bezeichnung `myVMFS`. Sie können die virtuelle Maschine so konfigurieren, dass diese virtuelle Festplatte verwendet wird, indem Sie die folgenden Zeilen zur Konfigurationsdatei der virtuellen Maschine hinzufügen:

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/myOS.vmdk
```

Migrieren von mit VMware Workstation und VMware GSX Server erstellten virtuellen Maschinen

Sie können den VI-Client nicht dazu verwenden, virtuelle Maschinen, die mit VMware Workstation oder VMware GSX Server angelegt wurden, in Ihr ESX Server 3-System zu migrieren. Sie können jedoch den Befehl `vmkfstools -i` dazu verwenden, die virtuelle Festplatte in Ihr ESX Server 3-System zu migrieren und diese Festplatte dann einer neuen virtuellen Maschine hinzufügen, die Sie in ESX Server 3 anlegen. Sie müssen die virtuelle Festplatte importieren, da Sie keine Festplatten einschalten können, die im Format `2gbsparse` auf einen ESX Server-Host exportiert wurden.

So migrieren Sie mit VMware Workstation und GSX Server erstellte virtuelle Maschinen

1 Importieren Sie eine Workstation- oder GSX Server-Festplatte in Ihr Verzeichnis `/vmfs/volumes/myVMFS/` oder ein beliebiges Unterverzeichnis.

2 Legen Sie im VI-Client eine neue virtuelle Maschine an, indem Sie die Konfigurationsoption **Benutzerdefiniert (Custom)** verwenden.

3 Wählen Sie beim Konfigurieren der Festplatte die Option **Vorhandene virtuelle Festplatte verwenden (Use an existing virtual disk)** aus, und fügen Sie die Workstation- oder GSX Server-Festplatte hinzu, die Sie importiert haben.

Erweitern einer virtuellen Festplatte

`-X --extendvirtualdisk <neue Größe>[kK|mM|gG]`

Diese Option erweitert die Größe einer Festplatte, die einer virtuellen Maschine zugewiesen wurde, nachdem die virtuelle Maschine erstellt wurde. Die virtuelle Maschine, die diese Festplattendatei verwendet, muss bei Eingabe dieses Befehls ausgeschaltet sein. Außerdem muss das Gastbetriebssystem in der Lage sein, die neue Festplattengröße zu erkennen und zu verwenden, damit es z. B. das Dateisystem auf der Festplatte aktualisieren kann, sodass der zusätzliche Speicherplatz auch genutzt wird.

Sie geben den Parameter `Neue Größe` in Kilobyte, Megabyte oder Gigbyte an, indem Sie das Suffix `k` (Kilobyte), `m` (Megabyte) oder `g` (Gigabyte) hinzufügen. Die Größeneinheit kann klein- oder großgeschrieben werden. `vmkfstools` interpretiert sowohl `k` als auch `K` als Kilobyte. Wenn Sie keine Einheit eingeben, ist die Standardeinstellung für `vmkfstools` Kilobyte.

Der Parameter `Neue Größe` beschreibt die gesamte neue Größe und nicht nur die beabsichtigte Erweiterung der Festplatte.

Um beispielsweise eine virtuelle Festplatte mit 4 GB um 1 GB zu erweitern, geben Sie Folgendes an:

```
vmkfstools -X 5g <Festplattenname>.dsk
```

HINWEIS Erweitern Sie nicht die Basisfestplatte einer virtuellen Maschine, der Snapshots zugeordnet sind. Falls doch, können Sie den Snapshot nicht länger übergeben oder die Basisfestplatte auf ihre ursprüngliche Größe zurücksetzen.

Migrieren einer VMFS-2 virtuellen Festplatte auf VMFS-3

```
-M --migratevirtualdisk
```

Diese Option konvertiert die angegebene virtuelle Festplattendatei vom Format ESX Server 2 ins Format ESX Server 3.

Anlegen einer Raw-Gerätezuordnung im virtuellen Kompatibilitätsmodus

```
-r --createrdm <Gerät>
```

Mit dieser Option wird eine Raw-Gerätezuordnungsdatei auf einem VMFS-3-Volume angelegt und eine Raw-Festplatte dieser Datei zugeordnet. Nach Herstellung dieser Zuordnung können Sie auf die Raw-Festplatten wie auf normale virtuelle VMFS-Festplatten zugreifen. Die Dateigröße der Zuordnung entspricht der Größe der Raw-Festplatte oder Partition, auf die sie verweist.

Bei der Angabe des Parameters `<Gerät>` geben Sie `0` für die Partition an, was bedeutet, dass die gesamte Raw-Festplatte verwendet wird. Wählen Sie das folgende Format:

```
/vmfs/devices/disks/vmhbaA:T:L:0
```

Weitere Informationen finden Sie unter „vmkfstools-Befehlssyntax“ auf Seite 300.

Weitere Informationen zum Konfigurieren von Raw-Gerätezuordnungen finden Sie unter „Raw-Gerätezuordnung“ auf Seite 155.

HINWEIS Alle Sperrmechanismen für VMFS-3-Dateien gelten auch für Raw-Gerätezuordnungen.

Beispiel der Erstellung einer Raw-Gerätezuordnung im virtuellen Kompatibilitätsmodus

```
vmkfstools -r /vmfs/devices/disks/vmhba1:3:0:0 my_rdm.vmdk
```

Das Beispiel zeigt die Erstellung einer Raw-Gerätezuordnungsdatei mit dem Namen `my_rdm.vmdk`, bei dem die Raw-Festplatte `vmhba1:3:0:0` dieser Datei zugeordnet wird. Sie können eine virtuelle Maschine so konfigurieren, dass sie die Zuordnungsdatei `my_rdm.vmdk` verwendet, indem Sie die Konfigurationsdatei der virtuellen Maschine um die folgenden Zeilen ergänzen:

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/my_rdm.vmdk
```

Anlegen einer Raw-Gerätezuordnung im physischen Kompatibilitätsmodus

`-z --createrdmpassthru <Gerät>`

Mit dieser Option können Sie einer Datei auf einem VMFS Volume ein Pass-Through-Raw-Gerät zuordnen. Bei dieser Zuordnung kann eine virtuelle Maschine die ESX Server 3-SCSI-Befehlsfilterung umgehen, wenn sie auf ihre virtuelle Festplatte zugreift. Diese Art der Zuordnung eignet sich dann, wenn die virtuelle Maschine systeminhärente SCSI-Befehle versenden muss, wie beispielsweise dann, wenn SAN-gestützte Software auf der virtuellen Maschine ausgeführt wird.

Nachdem Sie diese Art der Zuordnung aktiviert haben, können Sie damit auf die Raw-Festplatte wie auf jede andere virtuelle Festplatte zugreifen.

Bei der Angabe des Parameters `<Gerät>` geben Sie `0` für die Partition an, was darauf hinweist, dass das gesamte Raw-Gerät verwendet wird. Wählen Sie das folgende Format:

`/vmfs/devices/disks/vmhbaA:T:L:0`

Siehe „vmkfstools-Befehlssyntax“ auf Seite 300.

Aufführen der Attribute einer Raw-Gerätezuordnung

`-q --queryrdm`

Mit dieser Option können Sie die Attribute einer Raw-Festplattenzuordnung auflisten.

Diese Option druckt den „vmhba“-Namen der Raw-Festplatte „RDM“. Die Option druckt ferner weitere Identifikationsdaten wie die Festplatten-ID der Raw-Festplatte.

Anzeigen der Architektur der virtuellen Festplatte

`-g --geometry`

Mit dieser Option werden Informationen zur Architektur einer virtuellen Festplatte angezeigt.

Die Ausgabe erfolgt in dieser Form: `Architekturinformationen C/H/S`, wobei `C` die Anzahl der Zylinder, `H` die Anzahl der Köpfe und `S` die Anzahl der Sektoren angibt.

HINWEIS Beim Import virtueller Festplatten von VMware Workstation auf einen ESX Server 3-Host kann es zu Fehlermeldungen bezüglich Diskrepanzen in der Festplattenarchitektur kommen. Eine Diskrepanz in der Festplattenarchitektur kann auch die Ursache von Problemen beim Laden eines Gastbetriebssystems oder bei der Ausführung einer neu erstellten virtuellen Maschine sein.

Verwalten der SCSI-Reservierungen von LUNs

Die Option –L ermöglicht die Ausführung von Verwaltungsaufgaben für physische Speichergeräte. Sie können die meisten dieser Aufgaben auch über den VI-Client ausführen.

```
–L ––lock [reserve|release|lunreset|targetreset|busreset]<Gerät>
```

Mit dieser Option können Sie eine SCSI-LUN für die ausschließliche Verwendung durch einen ESX Server 3-Host reservieren, eine Reservierung aufheben, sodass andere Hosts auf die LUN zugreifen können, und eine Reservierung zurücksetzen, wodurch alle Reservierungen eines Ziels aufgehoben werden.

VORSICHT Eine Verwendung der Option –L kann den Betrieb der anderen Server in einem SAN beeinträchtigen. Verwenden Sie die Option –L nur zur Fehlerbehebung bei der Einrichtung von Clustern.

Wenden Sie diese Option nie auf eine LUN mit einem VMFS-Volume an, es sei denn, VMware empfiehlt Ihnen ausdrücklich das Gegenteil.

Sie können die Option –L auf verschiedene Arten anwenden:

- –L `reserve` – Reserviert die angegebene LUN. Nach der Reservierung kann nur der Server, der diese LUN reserviert hatte, darauf zugreifen. Wenn andere Server versuchen, auf diese LUN zuzugreifen, erhalten Sie einen Reservierungsfehler.
- –L `release` – Hebt die Reservierung der angegebenen LUN auf. Andere Server können wieder auf die LUN zugreifen.
- –L `lunreset` – Setzt die angegebene LUN zurück, indem jede Reservierung der LUN zurückgesetzt und die LUN den anderen Servern wieder zur Verfügung gestellt wird. Dies beeinflusst die anderen LUNs auf dem Gerät nicht. Wenn eine andere LUN auf dem Gerät reserviert wurde, bleibt sie reserviert.
- –L `targetreset` – Setzt das gesamte Ziel zurück. Dadurch werden die Reservierungen für alle LUNs, die dem Ziel zugeordnet sind, aufgehoben. Die–entsprechenden LUNs stehen wieder allen Servern zur Verfügung.
- –L `busreset` – Setzt alle zugänglichen Ziele auf dem Bus zurück. Dadurch werden die Reservierungen für alle LUNs, auf die durch den Bus zugegriffen werden kann, aufgehoben, und die entsprechenden LUNs stehen wieder allen Servern zur Verfügung.

Verwenden Sie für den Parameter `<Gerät>` folgendes Format:

```
/vmfs/devices/disks/vmhbaA:T:L:P
```

Siehe „vmkfstools-Befehlssyntax“ auf Seite 300.

Index

Symbole

* neben dem Pfad **151**

A

Administrator, Rolle **228**
Aktueller Multipathing-Status **149**
Ändern
  Benutzer auf ESX Server-Hosts **233**
  Gruppen auf ESX Server-Hosts **235**
  Kennwortverwendungsdauer für Benutzer und Gruppen **256**
  Kennwortverwendungsdauer für ESX Server **255**
  Proxy-Dienste für ESX Server **240**
  Servicekonsole, Kennwort-Plug-In **260**
  SSH-Konfiguration **266**
Anzeigen von ESX Server-Host-Benutzern und -Gruppen **231**
Ausfallstelle **110**
Authentifizierung
  Benutzer **224**
  Gruppen **225**
Authentifizierungs-Daemon **221**

B

Befehlsreferenz für ESX Server **291**
Benutzer
  ändern auf ESX Server-Hosts **233**
  Anzeigen der Benutzerliste **231**
  Authentifizierung **224**
  Benutzer mit direktem Zugriff **224**
  entfernen von ESX Server-Hosts **234**
  Exportieren einer Benutzerliste **231**
  hinzufügen zu In ESX Server-Hosts **232**
  in Windows-Domäne **224**
  Tabelle „Benutzer” für ESX Server-Hosts **230**
  VirtualCenter-Benutzer **224**
Berechtigungen
  Root-Benutzer **225**
  Übersicht **225**
  und Rechte **225**
  VirtualCenter-Administrator **225**
  vpxuser **225**
Bestimmen der Sicherheitsstufe der Servicekonsolen-Firewall **251**
Bevorzugter Pfad **151**, **153**
Blade-Server
  Konfigurieren eines VMkernel-Ports **83**
  Konfigurieren von Portgruppen virtueller Maschinen **82**
  und virtuelle Netzwerke **81**

C

CIM und Firewallports **198**

D

DAS-Firewallport für ESX Server **193**
Dateisysteme
  aktualisieren **143**
  NFS **95**

verwalten **142**
VMFS **95**
Datenspeicher
anzeigen im VI-Client **102**
erneut prüfen **134**
erstellen auf SCSI-Festplatte **110**
erstellen für Fibre-Channel-Geräte **114**
erstellen in hardwareinitiiertem iSCSI-Speicher **125**
erstellen in software-initiiertem iSCSI-Speicher **131**
Hinzufügen von Erweiterungen **145**
konfigurieren auf NFS-Volumes **137**
umbenennen **144**
und Dateisysteme **95**
verwalten **142**
Deaktivieren
Authentifizierung für iSCSI-Adapter **218**
Begrenzen der variablen Informationsgröße für Gastbetriebssystem **281**
Kopier- und Einfügevorgänge für Gastbetriebssysteme **277**
Protokollierung für Gastbetriebssysteme **282**, **286**
SSL für VI Web Access und SDK **238**
Delegierter Benutzer **242**, **244**
DHCP **39**
DNS **64**
Dynamische Erkennung **118**

E

Einrichten der CHAP-Authentifizierung für iSCSI-Adapter **217**
Einzelne Ausfallstelle **110**
Entfernen
Benutzer aus Gruppen **235**
Benutzer von ESX Server-Hosts **234**
Gruppen von ESX Server-Hosts **236**
Erweiterungen **145**
ESX Server
Ändern von Proxy-Diensten **240**
Architektur und Sicherheitsfunktionen **173**
Authentifizierung **221**
Authentifizierung für iSCSI-Speicher **214**
Befehlsreferenz **291**
Benutzer **221**
Delegierter Benutzer **242**
Hinzufügen von Benutzern **232**
Hinzufügen von Gruppen **235**
Host-zu-Host-Firewallports **198**
Implementierungen und Sicherheit **269**
Kennwortbeschränkungen **254**
Schlüsselqualität für Verbindungen **262**
Übersicht über die Sicherheit **173**
virtueller Switch, Sicherheit **207**
VLAN-Sicherheit **207**
ESX Server-Host-Kennwörter
Ändern des Plug-Ins **260**
Komplexität **256**
Konfigurieren der Kennwortkomplexität **259**
Konfigurieren von Regeln zur Wiederverwendung von Kennwörtern **259**
neue Kennwortkriterien **256**
Verwendungsdauer **255**
esxcfg-Befehle **291**
EUI-Bezeichner **117**
Exportieren von ESX Server-Host-

Benutzern und -Gruppen **231**

F

Failover **56**
Failover-Pfade
Status **150**
Festlegen der Sicherheitsstufe der Servicekonsolen-Firewall **251**
Feststehend, Pfadrichtlinie **146**
Fibre-Channel-Speicher
hinzufügen **114**
Übersicht **113**
Firewallports
Bestimmen der Sicherheitsstufe der Servicekonsolen-Firewall **251**
CIM **198**
Festlegen der Sicherheitsstufe der Servicekonsolen-Firewall **251**
freigeben und schließen für die Servicekonsole **252**
FTP **198**
für Verwaltungszugriff **193**
Herstellen einer Verbindung mit der VM-Konsole **196**
Host zu Host **198**
iSCSI-Software-Client **198**
Konfiguration mit VirtualCenter Server **189**
Konfiguration ohne VirtualCenter Server **191**
Lizenzserver und VirtualCenter Server **189**
NFS **198**
NIS **198**
öffnen mit dem VI-Client **198**
SDK und die Konsole für virtuellen Maschinen **196**
Servicekonsole **249**
Sicherheitsstufe **249**
Sicherungs-Agenten **249**
SMB **198**
SNMP **198**
SSH **198**
Übersicht **187**
und Verschlüsselung **236**
unterstützte Dienste **198**
Verwaltung **198**
VI Web Access und die Konsole für virtuelle Maschinen **196**
VI Web Access und VirtualCenter Server **189**
VI Web Access-Direktverbindung **191**
VI-Client und die Konsole für virtuelle Maschinen **196**
VI-Client und VirtualCenter Server **189**
VI-Client-Direktverbindung **191**
Freigeben von Ports in der Servicekonsolen-Firewall **252**
FTP und Firewallports **198**

G

Gastbetriebssysteme
Begrenzen der variablen Informationsgröße **281**
Deaktivieren der Protokollierung **282**, **286**
Deaktivieren von Kopier- und Einfügevorgängen **277**
Sicherheitsempfehlungen **276**
Gruppen
ändern auf ESX Server-Hosts **235**
Anzeigen der Gruppenliste **231**
Authentifizierung **225**
entfernen von ESX Server-Hosts **236**
Exportieren einer Gruppenliste **231**

hinzufügen zu In ESX Server-Hosts **235**
Tabelle „Gruppen” für ESX Server-Hosts **230**

H

Hardware-initiierter iSCSI-Speicher
hinzufügen **125**
Übersicht **119**
Hinzufügen
Benutzer zu ESX Server-Hosts **232**
Benutzer zu Gruppen **235**
Fibre-Channel-Speicher **114**
Gruppen zu ESX Server-Hosts **235**
Hardware-initiierter iSCSI-Speicher **125**
lokaler SCSI-Speicher **110**
NFS-Speicher **137**
Software-initiierter iSCSI-Speicher **131**
HTTP- und HTTPS-Firewallport **193**

I

Implementierungen für Sicherheit **269**
IQN-Bezeichner **117**
iSCSI
Authentifizierung **214**
CHAP **214**
Deaktivieren der Authentifizierung **218**
Firewallport für ESX Server **193**
Konfigurieren der CHAP-Authentifizierung **217**
Netzwerk **76**
QLogic-iSCSI-Adapter **214**
Schützen übertragener Daten **218**
Sicherheit **214**
Softwareclient und Firewallports **198**
Überprüfen der Authentifizierung **216**
iSCSI, Ports schützen **218**
iSCSI-HBA
Alias **121**
CHAP-Authentifizierung **124**
CHAP-Parameter **121**
dynamische Erkennung **121**
statische Erkennung **121**
iSCSI-Netzwerk
Erstellen einer Servicekonsolenverbindung **80**
Erstellen eines VMkernel-Ports **76**
iSCSI-Speicher
Erkennungsmethoden **118**
EUI-Bezeichner **117**
hardwareinitiiert **116**
Initiatoren **116**
IQN-Bezeichner **117**
Namensformate **117**
Sicherheit **118**
softwareinitiiert **116**
Isolierung
virtuelle Maschine **174**
virtuelle Netzwerkebene **179**
virtuelle Switches **179**
VLANs **179**

K

Kanonische Pfade **149**
Kein Zugriff, Rolle **228**
Kennwortbeschränkungen
für den ESX Server-Host **254**
Komplexität **256**
Mindestlänge **256**
Verwendungsdauer **255**
Kompatibilitätsmodi
physisch **161**
virtuell **161**

Konfigurieren
delegierter Benutzer **244**
ESX Server-Zertifikatssuchen **239**
Fibre-Channel-Speicher **114**
Hardware-initiierter iSCSI-Speicher **125**
Kennwortkomplexität **259**
lokaler SCSI-Speicher **110**
Multipathing für Fibre-Channel-Speicher **151**
Raw-Gerätezuordnung **165**
Regeln zur Wiederverwendung von Kennwörtern **259**
Software-initiierter iSCSI-Speicher **131**

L

Lastausgleich **56**
Lizenzserver
Firewallports für **193**
Firewallports mit VirtualCenter Server **189**
Lokaler SCSI-Speicher
hinzufügen **110**
Übersicht **110**

M

MAC-Adresse
generieren **69**
konfigurieren **70**
Multipathing
aktive Pfade **150**
ausgefallene Pfade **150**
deaktivierte Pfade **150**
Failover **151**
kanonische Pfade **149**
Standby-Pfade **150**
verwalten **151**
Multipathing-Richtlinie
einrichten **152**
Multipathing-Status **149**

N

NAS
Firewallport für ESX Server **193**
mounten **72**
Nessus **267**
Netzwerke
Sicherheit **203**
NFS
Delegierte Benutzer **242**
Firewallports **198**
NFS-Speicher
hinzufügen **137**
Übersicht **135**
NIC-Gruppierung
Definition **20**
NIS und Firewallports **198**
Nur lesen, Rolle **228**

O

Optimale Vorgehensweisen für Netzwerke **72**

P

pam_cracklib.so, Plug-In **256**
pam_passwdqc.so, Plug-In **260**
Pfadausfall **146**
Pfade
bevorzugt **151**, **153**
Pfade verwalten, Dialogfeld **153**
Pfadrichtlinien
Feststehend **146**
Round Robin **147**
Zuletzt verwendet **146**
Portgruppe
Definition **20**
konfigurieren **60**
verwenden **24**

Proxy-Dienste
ändern **240**
und Verschlüsselung **236**

R

Raw-Gerätezuordnung
Dynamische Namensauflösung **163**
erstellen **165**
Gerätezuordnungen **156**
mit Cluster **164**
physischer Kompatibilitätsmodus **161**
und virtuelle Festplattendateien **165**
und vmkfstools **169**
virtueller Kompatibilitätsmodus **161**
Raw-Gerätezuordnungen
Übersicht **156**
Vorteile **157**
Rechte
und Berechtigungen **225**
Ressourcenbegrenzung und Sicherheit **174**
Ressourcengarantien und Sicherheit **174**
Richtlinie zur Unterstützung von Drittanbieter-Software **186**
Rollen
Administrator **228**
Kein Zugriff **228**
Nur Lesen **228**
Standard **228**
und Berechtigungen **228**
Root-Anmeldung
Berechtigungen **225**
Delegierter Benutzer **242**
SSH **265**
Round Robin, Pfadrichtlinie **147**
Routing **64**
RPMs **267**

S

Schicht 2-Sicherheit **52**
Schließen von Ports in der Servicekonsolen-Firewall **252**
SCSI
vmkfstools **299**
SDL und Firewallports zum Herstellen einer Verbindung mit der VM-Konsole **196**
Servicekonsole
absichern mit VLANs und virtuellen Switches **207**
Anmeldung **249**
Direkte Verbindungen **249**
Empfehlungen für den Schutz **248**
Kennwortbeschränkungen **254**
Remoteverbindungen **249**
setgid-Anwendungen **263**
setuid-Anwendungen **263**
Sicherheit **177**
SSH-Verbindungen **265**
Servicekonsole, Netzwerk
Fehlerbehebung **85**
Konfiguration **34**
setgid-Anwendungen **263**
setuid-Anwendungen **263**
Sicherheit
Beispiel, DMZ auf einem einzelnen ESX Server-Host **180**, **181**
Benutzer mit direktem Zugriff **224**
Benutzerauthentifizierung **221**
Benutzerverwaltung **221**
Berechtigungen **225**
CHAP-Authentifizierung **214**
Delegierter Benutzer **242**
Empfehlungen für virtuelle Maschinen **276**
ESX Server-Architektur **173**
Gefälschte Übertragungen **211**

Gruppen **225**
iSCSI-Speicher **214**
Kennwortbeschränkungen für den ESX Server-Host **254**
MAC-Adressenänderungen **211**
PAM-Authentifizierung **221**
Patches **267**
Promiscuous-Modus **211**
Rollen **228**
Schlüsselqualität **262**
Servicekonsole, Sicherheitsmaßnahmen **1 77**
Servicekonsolen-Firewall, Sicherheitsstufe **249**
setgid-Anwendungen **263**
setuid-Anwendungen **263**
Sicherheitszertifikate **236**
SSH-Verbindungen **265**
Übersicht über Benutzer, Gruppen, Berechtigungen und Suchsoftware **267**
Verschlüsselung **236**
VirtualCenter-Benutzer **224**
Virtualisierungsebene **174**
virtuelle Maschinen **174**
virtuelle Netzwerkebene **179**
virtuelles Netzwerk **203**
VLAN-Hopping **207**
VLANs **203**
VMkernel **174**
vmware-authd **221**
VMware-Richtlinie **186**
Rollen **223**
SMB und Firewallports **198**
SNMP und Firewallports **198**
Software-initiierter iSCSI-Speicher
hinzufügen **131**
Übersicht **127**
Speicher
absichern mit VLANs und virtuellen Switches **207**
Adapter **95**
anzeigen im VI-Client **102**
Fibre-Channel **113**
iSCSI **116**
Konfigurationsaufgaben **106**
lokaler SCSI- **110**
NFS **135**
SAN **113**
Typen **93**
Zugriff für virtuelle Maschinen **100**
Speicheradapter
anzeigen im VI-Client **104**
erneut prüfen **134**
Fibre-Channel **113**
iSCSI-HBA **121**
SSH
Ändern der Konfiguration **266**
Firewallports **198**
Sicherheitseinstellungen **265**
Statische Erkennung **118**
Sternchen neben dem Pfad **151**

T

TCP-Ports **193**
Tomcat, Webdienst **177**
Traffic-Shaping **54**

U

Überprüfen der Authentifizierung für iSCSI-Adapter **216**
UDP-Ports **193**

V

Verhindern der böswilligen Gerätetrennung **279**
Verschlüsselung
für Benutzernamen, Kennwörter und Pakete **236**

- und Aktivieren und Deaktivieren von SSL **236**

Verwaltungszugriff
- Firewallports **193**

VI Web Access
- Deaktivieren von SSL **238**
- Firewallports für Direktverbindung **191**
- Firewallports mit VirtualCenter Server **189**
- Firewallports zum Herstellen einer Verbindung mit der VM-Konsole **196**
- und ESX Server-Dienste **236**

VI-Client
- Firewallports für Direktverbindung **191**
- Firewallports mit VirtualCenter Server **189**
- Firewallports zum Herstellen einer Verbindung mit der VM-Konsole **196**

VirtualCenter Server
- Berechtigungen **225**
- Firewallports **189**

Virtualisierungsebene und Sicherheit **174**

Virtuelle Maschine, Netzwerke **27**

Virtuelle Maschinen
- Begrenzen der variablen Informationsgröße **281**
- Deaktivieren der Protokollierung **282**, **286**
- Deaktivieren von Kopier- und Einfügevorgängen **277**
- Delegierter Benutzer **242**
- konfigurieren eines delegierten Benutzers **244**
- Ressourcenreservierung und -einschränkungen **174**
- Sicherheit **174**
- Sicherheitsempfehlungen **276**
- Verhindern der Gerätetrennung **279**

virtuelle Maschinen
- Beispiel für die Isolierung **180**, **181**

Virtuelle Netzwerkebene und Sicherheit **179**

Virtuelle Switches
- Angriffe durch 802.1q- und ISL-Kennzeichnung **209**
- Doppelt eingekapselte Angriffe **209**
- Gefälschte Übertragungen **211**
- Implementierungsszenarien **269**
- MAC-Adressenänderungen **211**
- MAC-Flooding **209**
- Multicast-Brute-Force-Angriffe **209**
- Promiscuous-Modus **211**
- Sicherheit **209**
- Spanning-Tree-Angriffe **209**
- und iSCSI **218**
- Zufallsdatenblock-Angriffe **209**

VLAN
- Definition **20**

VLANs
- Implementierungsszenarien **269**
- Schicht 2-Sicherheit **207**
- Sicherheit **203**
- und iSCSI **218**
- VLAN-Hopping **207**

VMFS
- gemeinsam nutzen **269**
- vmkfstools **299**

VMkernel
- Definition **20**
- konfigurieren **30**
- Sicherheit **174**

vmkfstools
- Dateisystemoptionen **301**
- Optionen für virtuelle Festplatten **305**

Syntax **300**
Übersicht **299**
VMotion
absichern mit VLANs und virtuellen Switches **207**
Definition **20**
Firewallport **193**
Netzwerkkonfiguration **30**
vSwitch
Definition **20**
Richtlinien **51**
verwenden **22**

Z

Zertifikate
Deaktivieren von SSL für VI Web Access und SDK **238**
Konfigurieren von ESX Server-Suchen **239**
Schlüsseldatei **236**
Speicherort **236**
Zertifikatsdatei **236**
Zertifizierung **186**
Zugriff auf Speicher **100**
Zuletzt verwendet, Pfadrichtlinie **146**